(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 65 668 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 100 65 668.4
(22) Anmeldetag: 29. 12. 2000
(43) Offenlegungstag: 9. 8. 2001

DE 100 65 668 A 1

(30) Unionspriorität:
476594 31. 12. 1999 US

(71) Anmelder:
GE Medical Technology Services, INC., Pewaukee, Wisconsin, US

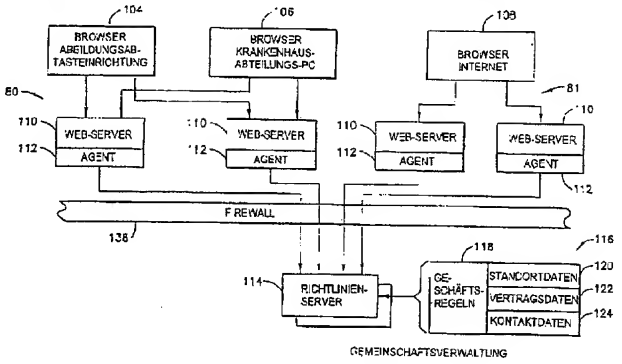
(74) Vertreter:
Tiedtke, Bühling, Kinne & Partner, 80336 München

(72) Erfinder:
Zettel, Hubert Anthony, Waukesha, Wis., US; Mehring, David Thomas, Sussex, Wis., US; Palliyal, Sunil Melepatt, Kerala, IN; Lamoureaux, Thomas Leroy, Waukesha, Wis., US; Hummel jun., Henry John, Waukesha, Wis., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und Vorrichtung zum sicheren Fernzugriff auf Software bei einer zentralen Dienstanlage

(57) Die Erfindung stellt ein Verfahren und ein System zur Zustellung geschützter Softwareanwendungen von einer zentralen Dienstanlage (22) zu entfernten Systemen (12) bereit, wobei die Zustellung auf der Grundlage der Gemeinschaftsmitgliedschaft des Benutzers eines entfernten Systems verwaltet wird. Es werden Geschäftsregeln (118) verwendet, um zu bestimmen, ob ein spezieller beglaubigter Benutzer, der einen Zugriff auf eine geschützte Softwareanwendung von einem speziellen entfernten Standort anstrebt, berechtigt werden soll. Eine Vielzahl von Web-Servern (110) ist dazu programmiert, einen selektiven Zugriff auf eine residente Softwareanwendung oder mehrere residente Softwareanwendungen durch Benutzer eines entfernten Systems über ein Netz (80) zu ermöglichen. Der Zugriff wird durch einen zentralen Richtlinien-Server (114) basierend auf Benutzer- und Systeminformationen sowie Gemeinschaftsdefinitionen, die in einer Datenbank (116) gespeichert sind, verwaltet. Der Richtlinien-Server kommuniziert mit jedem Web-Server über ein in dem Web-Server enthaltenes Agenturmodul (112). Das Agenturmodul fängt Anforderungen zum Zugriff von Benutzern eines entfernten Systems ab und verbindet sich daraufhin mit dem Richtlinien-Server. Der Richtlinien-Server beglaubigt Kennwörter, während er die Beglaubigung zugeordneter Sicherheitscodes an einen Sicherheits-Server (126) übergibt. Falls das Kennwort und der Sicherheitscode beglaubigt werden, wendet der Richtlinien-Server daraufhin die ...



DE 100 65 668 A 1

Beschreibung

Die Erfindung bezieht sich allgemein auf den Softwareschutz und die Lizenzüberwachung von Anwendungssoftware und Informationsdateien für Fernanwendungen.

Die Fernüberwachung und -diagnose von Ausstattung oder Systemen stellt ein Beispiel für eine Fernanwendung dar. Derzeit entwickeln viele Firmen Fähigkeiten zur Fernüberwachung und -diagnose von Ausstattung oder Systemen. Die entfernte Ausstattung oder die entfernten Systeme (auf die nachstehend als entfernte Systeme Bezug genommen ist) umfassen die Skala von industriellen Dampfturbinen bis zu vernetzten Druckern, von medizinischer Abbildungsausstattung bis zu Haushaltsgeräten. In beinahe allen Fällen befindet sich eine gewisse Rechenfähigkeit bei den entfernten Systemen wie beispielsweise eine Verarbeitungseinrichtung. Im allgemeinen führt die Verarbeitungseinrichtung Funktionen aus wie beispielsweise eine Datenerfassung, eine Betriebsüberwachung, eine Ausführung von Diagnoseanwendungen und eine Bereitstellung eines Zugriffs auf Informationen und Anwendungen bei den entfernten Systemen für den Endbenutzer oder Kunden.

Bei einer typischen Fernüberwachungsanwendung können bei einem entfernten System befindliche Software und andere Informationsdateien nicht durch den Lieferanten direkt kontrolliert werden, da sie sich in der Umgebung des Kunden befinden. Einige der Softwareanwendungen und Informationsdateien in der Verarbeitungsumgebung sind jedoch hochempfindlich und müssen vor einer Manipulation (z. B. einer versehentlichen Modifikation und einer böswilligen Beschädigung) geschützt werden. Eine Manipulation bei Softwareanwendungen oder Informationsdateien wie beispielsweise bei dem entfernten System befindlichen Konfigurationsdateien kann einen Benutzer daran hindern, auf eine benötigte Funktionalität zuzugreifen. Alternativ kann es eine Manipulation einem Benutzer ermöglichen, auf eine beschränkte Funktionalität zuzugreifen. Es ist sogar möglich, daß eine Manipulation zu einer Störung der Ausstattung führen kann.

Daher sind Systeme zum Schutz von bei einem entfernten System befindlichen Softwareanwendungen und Konfigurationsinformationsdateien vor einer Manipulation bekannt. Ein bekanntes System verwendet Mechanismen zur Sicherstellung, daß auf Dateien von einem Kunden, der nicht für sie bezahlt hat und dessen Zugriff beendet wurde, nicht zugegriffen werden kann. Diese Mechanismen stellen ebenfalls sicher, daß nicht mit dem Lieferanten übereinstimmende Dienstleister, die Dienste bei dem entfernten System vornehmen können, nicht auf Diagnosedienstprogramme zugreifen können.

Typischerweise führen befugte Außendiensttechniker Dienstbesuche bei entfernten Standorten zum Zwecke des Vornehmens von Diensten bei Ausstattung an den Standorten aus. Während er sich im Außendienst befindet, kann der Außendiensttechniker unter Verwendung einer Außendiensteinheit über ein Netz mit einer zentralen Dienstanlage kommunizieren. Die Außendiensteinheit kann einen zur Verwendung durch Außendiensttechniker an entfernten Standorten entworfenen tragbaren Computer aufweisen. Die Einheit umfaßt eine Dienstplattform, die gewisse funktionelle Schaltungen zur Begründung einer einheitlichen Dienstgrundlage für die entfernten Systeme aufweist. Ferner umfassen die Diensteinheiten spezifische Diensthilfseinrichtungen, die es dem Außendiensttechniker ermöglichen, Ferndienstnachrichten, Berichte über spezifische Diagnosesysteme, Dienstpläne usw. anzufordern und zu empfangen. Durch die Dienstplattform kann der Außendiensttechniker auf Systemkonfigurationen, historische Protokollinformationen, Systemnetzinformationen, Analyseprotokolle und -daten usw. zugreifen. Der Außendiensttechniker kann auch Dienstaufzeichnungen aktualisieren. Typischerweise ist die Außendiensteinheit mit einem Zugriffsmodul programmiert, um es der Dienstanlage zu ermöglichen, den Lizenz- und Sicherheitsstatus der Außendiensteinheit zu verifizieren. Beispielsweise kann es das Zugriffsmodul in Zusammenarbeit mit Schaltungen bei der Dienstanlage einem Außendiensttechniker ermöglichen, auf Daten oder Anwendungen zuzugreifen, die einen Teil der Funktionalität oder die gesamte Funktionalität bereitstellen, die Außendiensttechnikern bei der Dienstanlage angeboten wird. Derartige Funktionalitäten können denen ähneln, die bei den entfernten Systemen selbst bereitgestellt sind, oder können dem Außendiensttechniker ein breiteres Spektrum von Dienstoptionen anbieten. Insbesondere kann die Außendiensteinheit mit Dienstanwendungen ausgestattet sein wie beispielsweise Dienstanwendungen zur Analyse von Diagnosesystemleistungsdaten, zur Planung regulärer oder spezieller Dienstbesuche, zur Planung einer Versendung von Ersatzteilen usw.. Andere Anwendungen können es dem Außendiensttechniker ermöglichen, sich mit Dienstanforderungen von dem entfernten System zu befassen sowie Dienstnachrichten und -aktualisierungen über die Außendiensteinheit zu übertragen. Die Außendiensteinheiten können Personal-Computer oder Laptop-Computer von jeder geeigneten Prozessorplattform umfassen.

Offensichtlich benötigen befugte Außendiensttechniker einen Zugriff auf andere Softwareanwendungen als die Softwareanwendungen, auf die von anderen Systembenutzern zugegriffen wird. Insbesondere benötigt der Außendiensttechniker einen Zugriff auf proprietäre und sehr empfindliche Software in der Form von Diensthilfseinrichtungen, Dienstdokumentation und Dienstaufzeichnungen, um ein Systemprobleme lösendes und gutes Vornehmen von Diensten bei Ausstattung zu ermöglichen. Es ist im Geschäftsinteresse des Betreibers der zentralen Dienstanlage, den Zugriff auf proprietäre und sehr empfindliche Software auf befugte Einzelpersonen, d. h. auf Personen mit der erforderlichen Sicherheitsfreigabe, zu beschränken. Vorzugsweise ermöglicht es ein Sicherheitssystem Außendienstpersonal und anderen befugten Personen von dem entfernten System, bei dem Dienste vorgenommen werden, auf zentrale Software einer sehr empfindlichen Natur zuzugreifen, während es andere befugte Benutzer, denen die erforderliche Sicherheitsfreigabe fehlt, an einem Zugriff auf die gleiche Software hindert.

Somit besteht ein Bedarf an einem System zur Bereitstellung einer breiten Vielfalt von Softwareanwendungen für eine breite Vielfalt von Gemeinschaften von Benutzern eines entfernten Systems auf der Grundlage unterschiedlicher Sicherheitsstufen. In dem Fall, in dem eine Geschäftseinheit wie beispielsweise ein Krankenhaus über einen Dienstvertrag mit einem Lieferanten verfügt, der einen Dienst vor Ort und einen Zugriff von einem entfernten Standort auf bei einer zentralen Anlage befindliche Softwareanwendungen bereitstellt, besteht ein Bedarf an einem Verfahren zur Verwaltung eines Fernzugriffs auf die Software durch Benutzer mit unterschiedlichen Sicherheitsklassifikationen. Das System sollte ferner dazu in der Lage sein, unterschiedliche Zugriffsrechte für verschiedene Personen mit der gleichen Sicherheitsfreigabe bereitzustellen. Beispielsweise sollten in jeder Sicherheitsstufe die Benutzer basierend auf unterschiedlichen Befugnisstufen und unterschiedlichen Stellenverantwortlichkeiten (d. h. einer Mitgliedschaft in verschiedenen Gemeinschaften), die den Bedarf zum Zugriff auf unterschiedliche eine spezielle Sicherheitsstufe erfordernde Softwareanwendungen verursachen, weiter unterschieden

werden.

Die Erfindung ist auf ein Verfahren und ein System zur Zustellung geschützter Softwareanwendungen von einer zentralen Dienstanlage zu entfernten Systemen gerichtet, wobei die Zustellung auf der Grundlage der Sicherheitsfreigabestufe und auf der Grundlage der Gemeinschaftsmitgliedschaft des Benutzers eines entfernten Systems verwaltet wird. Es wird ein Sicherheitsschema mit zwei Faktoren verwendet, um zu bestimmen, ob Benutzer eines entfernten Systems, die einen Zugriff auf mit einer hohen Stufe geschützte Softwareanwendungen anstreben, glaubwürdig sind. Es werden Geschäftsregeln zur Bestimmung, ob einen Zugriff anstrebende beglaubigte Benutzer berechtigt werden sollen, verwendet.

Gemäß den bevorzugten Ausführungsbeispielen der Erfindung ist eine Vielzahl von Web-Servern dazu programmiert, einen selektiven Zugriff auf eine residente Softwareanwendung oder mehrere residente Softwareanwendungen durch Benutzer eines entfernten Systems über ein Netz zu ermöglichen. Einige Anwendungen sind offen, und andere Anwendungen sind geschützt, wobei vorzugsweise zwei Stufen des Schutzes auferlegt werden. Der Zugriff wird durch einen zentralen Richtlinien-Server basierend auf Benutzer- und Systeminformationen sowie Gemeinschaftsdefinitionen, die in einer Datenbank gespeichert sind, verwaltet. Der Richtlinien-Server kommuniziert mit jedem Web-Server über ein in dem Web-Server enthaltenes Agenturmodul.

Das Agenturmodul fängt Anforderungen zum Zugriff von Benutzern eines entfernten Systems ab und verbindet sich mit dem Richtlinien-Server. Das Agenturmodul bestimmt, ob die angeforderte Anwendung offen oder geschützt ist. Falls die angeforderte Softwareanwendung offen ist, signalisiert das Agenturmodul es dem Web-Server, den Zugriff zu ermöglichen. Falls die angeforderte Softwareanwendung geschützt ist, kontaktiert das Agenturmodul den Richtlinien-Server. Der Richtlinien-Server beglaubigt Kennwörter, während er die Beglaubigung zugeordneter Sicherheitscodes an einen Sicherheits-Server übergibt. Falls das Kennwort und der Sicherheitscode beglaubigt werden, wendet der Richtlinien-Server daraufhin die Geschäftsregeln an, um zu bestimmen, ob der anfordernde Benutzer eines entfernten Systems dazu befugt ist, auf die geschützte Softwareanwendung zuzugreifen.

Gemäß dem bevorzugten Ausführungsbeispiel wird ein Zugriff auf strenger geschützte Softwareanwendungen ermöglicht, falls ein Sicherheitstest mit zwei Faktoren erfüllt wird. Jeder Benutzer mit einer derartigen Sicherheitsfreigabe einer hohen Stufe muß sowohl ein geheimes Kennwort als auch eine zufällig erzeugte Sicherheitscodezahl bereitstellen. Falls das Kennwort und der Sicherheitscode glaubwürdig sind, werden daraufhin Benutzer-, Standort-, System- und Vertragsinformationen sowie Geschäftsregeln zur Bestimmung, ob der Benutzer eines entfernten Systems einer Gemeinschaft mit Zugriffsrechten für die streng geschützte Software angehört, verwendet. Eine spezielle Einzelperson kann gleichzeitig Mitglied verschiedener Gemeinschaften sein.

Gemäß dem bevorzugten Ausführungsbeispiel der Erfindung werden abhängig davon, ob der Benutzer eine Sicherheitsfreigabe mit einem Faktor oder mit zwei Faktoren aufweist, unterschiedliche Benutzerbeglaubigungsalgorithmen verwendet. Benutzer mit einer Sicherheitsfreigabe mit einem Faktor sind berechtigt, auf Softwareanwendungen mit einer niedrigen Stufe des Schutzes zuzugreifen, während die Benutzer mit einer Sicherheitsfreigabe mit zwei Faktoren berechtigt sind, sowohl auf mit einer niedrigen Stufe geschützte als auch auf mit einer hohen Stufe geschützte Softwareanwendungen zuzugreifen. Vorzugsweise überträgt der spezielle Benutzer eines entfernten Systems eine Anforderung zum Zugriff auf eine spezielle Softwareanwendung über einen Web-Browser bei dem entfernten System, wobei letzterer über ein Netz mit dem Web-Server verbunden ist, bei dem sich die angeforderte Softwareanwendung befindet. Falls der Benutzer eine Sicherheitsfreigabe mit zwei Faktoren aufweist, muß er/sie während einer Anmeldung beide Faktoren wie beispielsweise ein Kennwort und einen Sicherheitscode zusätzlich zu einer Benutzeridentifizierung eingeben. Vorzugsweise wird die Sicherheitszahl von einer durch den Benutzer getragenen Zufallszahlenerzeugungseinrichtung erhalten, die vorher mit einer eindeutigen Keimzahl (seed number) geladen wurde. Die eindeutige Keimzahl und die Zeit, zu der die Zufallszahlenerzeugung aktiviert wurde, werden in Verbindung mit dem Benutzernamen und dem Kennwort für die Einzelperson in einer zentralen Benutzerdatenbank gespeichert. Wenn der Benutzer lediglich eine Sicherheitsfreigabe mit einem Faktor aufweist, dann werden während einer Anmeldung lediglich der eine Faktor (z. B. ein Kennwort) und die Benutzeridentifizierung eingegeben.

In jedem Fall fängt das Agenturmodul für den Web-Server, bei dem sich die angeforderte Software befindet, die Anforderung zum Zugriff und die angemeldeten Benutzerinformationen ab und leitet sie daraufhin zu dem zentralen Richtlinien-Server weiter. Vorzugsweise sind die verteilten Web-Server durch eine Firewall von dem zentralen Richtlinien-Server getrennt. Die übertragenen Informationen werden zur Bestimmung, ob die Anforderung zum Zugriff genehmigt werden soll, von dem Richtlinien-Server verarbeitet. Diese Verarbeitung umfaßt zwei Stufen: (1) Beglaubigung des Benutzers; und (2) Genehmigung zum Zugriff auf die angeforderte Softwareanwendung. Der Richtlinien-Server beglaubigt das Kennwort, indem er Bezug auf eine Gemeinschaftsverwaltungsdatenbank nimmt, auf die elektronisch zugegriffen werden kann. Der Richtlinien-Server gewinnt ferner Sicherheitsinformationen aus der Gemeinschaftsverwaltungsdatenbank wieder, die von dem Sicherheits-Server zur Beglaubigung des für die Sicherheitsfreigabe mit zwei Faktoren erforderlichen Sicherheitscodes verwendet werden. Falls das Kennwort und der Sicherheitscode glaubwürdig sind, fährt der Richtlinien-Server daraufhin basierend auf Benutzer-, Standort-, System- und Vertragsinformationen sowie anderen Informationen und Geschäftsregeln (d. h. Gemeinschaftsdefinitionen) in der Gemeinschaftsverwaltungsdatenbank fort, zu bestimmen, ob der Zugriff genehmigt werden soll. Die Geschäftsregeln wenden gewisse Kriterien an, um zu bestimmen, ob die spezielle Gemeinschaft, der der Benutzer angehört, zum Zugriff auf die angeforderten geschützten Softwareanwendungen befugt ist.

In Fällen, in denen eine Sicherheitsfreigabe mit zwei Faktoren erforderlich ist, gewinnt der Richtlinien-Server, falls der Benutzername und das Kennwort glaubwürdig sind, eine Keimzahl und eine Zahlenerzeugungsanfangszeit aus der Datenbank wieder und überträgt sie zu dem Sicherheits-Server. Der Sicherheits-Server berechnet daraufhin unter Verwendung der Zahlenerzeugungsanfangszeit und des gleichen Zufallszahlenerzeugungsalgorithmus, wie er von der Zufallszahlenerzeugungseinrichtung des Benutzers eines entfernten Systems verwendet wird, eine Sicherheitszahl aus der Keimzahl. Falls die von dem Benutzer eingegebene Sicherheitszahl sich in einem vorbestimmten Bereich der von dem Sicherheits-Server erzeugten Sicherheitszahl befindet, überträgt der Sicherheits-Server ein Signal zu dem Richtlinien-Server, das angibt, daß die Sicherheitszahl glaubwürdig ist. Falls eine Sicherheitsfreigabe mit zwei Faktoren erforderlich ist, beglaubigt somit der Richtlinien-Server das geheime Kennwort, während der Sicherheits-

Server den Sicherheitscode beglaubigt. Für Fälle, in denen eine Sicherheitsfreigabe mit einem Faktor erforderlich ist, beglaubigt der Richtlinien-Server das Kennwort ohne eine Bezugnahme auf den Sicherheits-Server.

Im Anschluß an die Beglaubigung bestimmt der Richtlinien-Server daraufhin, ob der Benutzer Mitglied einer Gemeinschaft von Benutzern ist, die dazu befugt ist, auf die angeforderte Softwareanwendung zuzugreifen. Zur Ausführung dieser Bestimmung muß der Richtlinien-Server wieder Informationen aus der Gemeinschaftsverwaltungsdatenbank wie beispielsweise Benutzerstatusinformationen, Standortinformationen, Systeminformationen, Vetragsinformationen und Geschäftsregeln wiedergewinnen. Wenn der Benutzer nicht Mitglied einer Gemeinschaft mit Zugriffsrechten ist, dann wird dem Benutzer der Zugriff auf die angeforderte Softwareanwendung verweigert. Alternativ wird der Zugriff gestattet, falls der anfordernde Benutzer eines entfernten Systems Mitglied einer Gemeinschaft mit Zugriffsrechten für die angeforderte Softwareanwendung ist.

Es zeigen:

Fig. 1 eine schematische Darstellung einer Reihe von medizinischen Diagnosesystemen, die über eine Netzverbindung zur Bereitstellung eines zentralisierten Dienstes und eines Datenaustauschs zwischen den Diagnosesystemen und der Dienstanlage mit einer Dienstanlage gekoppelt sind;

Fig. 2 ein Blockschaltbild der in **Fig.** 1 gezeigten Systeme, das gewisse funktionelle Komponenten der Diagnosesysteme und der Dienstanlage veranschaulicht;

Fig. 3 ein Blockschaltbild, das die funktionellen Komponenten einer zur Verwendung bei einem entfernten System geeigneten einheitlichen Dienstplattform zeigt;

Fig. 4 ein Blockschaltbild, das Teile eines Gemeinschaftsverwaltungssystems gemäß dem bevorzugten Ausführungsbeispiel der Erfindung zeigt;

Fig. 5 ein Blockschaltbild, das Teile eines Systems zur Gemeinschaftsverwaltung eines Fernzugriffs mit einer Sicherheitsfreigabe gemäß dem bevorzugten Ausführungsbeispiel der Erfindung zeigt;

Fig. 6 ein Flußdiagramm, das den sicheren Gemeinschaftsverwaltungsprozeß gemäß dem bevorzugten Ausführungsbeispiel der Erfindung allgemein darstellt; und

Fig. 7 ein Blockschaltbild, das ein Hybridsystem zeigt, das das bevorzugte Ausführungsbeispiel der Erfindung mit dem in **Fig.** 1 und 2 dargestellten bekannten System kombiniert.

Die nachstehende ausführliche Beschreibung des bevorzugten Ausführungsbeispiels der Erfindung ist in dem Zusammenhang einer zentralen Anlage zum Vornehmen von Diensten bei einer Vielzahl von entfernt angeordneten medizinischen Diagnosesystemen und Workstations über ein Netz dargestellt. Es sollte jedoch erkannt werden, daß die Erfindung bei jedem System Anwendung findet, bei dem entfernte Systeme lizenzierte Software und/oder Datenbankdateien verwenden und über ein Netz mit einer zentralen Anlage verbunden sind.

Auf **Fig.** 1 Bezug nehmend ist ein Dienstsystem **10** gemäß dem Stand der Technik zur Bereitstellung eines zentralisierten Dienstes für eine Vielzahl von entfernt angeordneten medizinischen Diagnosesystemen **12** veranschaulicht. Bei dem in **Fig.** 1 gezeigten Ausführungsbeispiel umfassen die medizinischen Diagnosesysteme ein Kernspintomographiesystem (MRI-System) **14**, ein Computertomographiesystem (CT-System) **16** und ein Ultraschallabbildungssystem **18**. Die Diagnosesysteme können bei einem einzigen Ort oder einer einzigen Anlage wie beispielsweise einer medizinischen Anlage **20** positioniert sein oder können voneinander entfernt sein, wie es in dem Fall des Ultraschallsystems **18** gezeigt ist. Die Diagnosesysteme werden von einer zentralisierten Dienstanlage **22** mit Diensten versehen. Ferner kann eine Vielzahl von Außendiensteinheiten (FE) **24** zur Übertragung von Dienstanforderungen, Verifikation des Dienststatus, Übertragung von Dienstdaten usw. mit dem Dienstsystem gekoppelt sein, wie es nachstehend ausführlicher beschrieben ist.

Abhängig von der Modalität der Systeme sind verschiedene Subkomponenten oder Subsysteme enthalten. Im Falle des MRI-Systems **14** umfassen derartige Systeme im allgemeinen eine Abtasteinrichtung **26** zur Erzeugung gepulster Magnetfelder und zur Sammlung von Signalen von Emissionen durch gyromagnetisches Material in einem Objekt von Interesse. Die Abtasteinrichtung ist mit einer Steuer- und Signalerfassungsschaltung **28** gekoppelt, die ihrerseits mit einer Systemsteuereinrichtung **30** gekoppelt ist. Die Systemsteuereinrichtung **30** umfaßt eine einheitliche Plattform zum interaktiven Austausch von Dienstanforderungen, Nachrichten und Daten mit der Dienstanlage **22**, wie es nachstehend ausführlicher beschrieben ist. Die Systemsteuereinrichtung **30** ist mit einem Kommunikationsmodul **32** verbunden, das in einer einzigen oder getrennten physischen Baueinheit von der Systemsteuereinrichtung **30** enthalten sein kann. Die Systemsteuereinrichtung **30** ist auch mit einer Bedienungspersonstation **34** verbunden, die typischerweise einen Computermonitor **36**, eine Tastatur **38** sowie andere Eingabevorrichtungen **40** wie beispielsweise eine Maus umfaßt. Bei einem typischen System können zusätzliche Komponenten in dem System **14** enthalten sein wie beispielsweise ein Drucker oder ein fotografisches System zur Erzeugung rekonstruierter Bilder basierend auf von der Abtasteinrichtung **14** gesammelten Daten.

Ähnlich umfaßt das CT-System **16** typischerweise eine Abtasteinrichtung, die Teile von durch ein Objekt von Interesse gerichteter Röntgenstrahlung erfaßt. Die Abtasteinrichtung **42** ist mit einer Erzeugungs- und Steuereinrichtung sowie mit einer Signalerfassungseinheit zur Steuerung des Betriebs einer Röntgenquelle und eines Portals in der Abtasteinrichtung **42** und zum Empfangen von durch eine in der Abtasteinrichtung bewegbare regelmäßige Anordnung von Detektoren erzeugten Signalen gekoppelt, die bei dem Bezugszeichen **44** zusammengefaßt dargestellt sind. Die Schaltungen in den Steuer- und Signalerfassungskomponenten sind mit einer Systemsteuereinrichtung **46** gekoppelt, die wie die vorstehend angeführte Steuereinrichtung **30** Schaltungen zur Befehligung des Betriebs der Abtasteinrichtung sowie zur Verarbeitung und Rekonstruktion von Bilddaten basierend auf den erfaßten Signalen umfaßt. Die Systemsteuereinrichtung **46** ist mit einem im allgemeinen dem Kommunikationsmodul **32** des MRI-Systems **14** ähnelnden Kommunikationsmodul **48** zum Senden und Empfangen von Daten für einen zentralen Dienst bei dem System **16** verbunden. Die Systemsteuereinrichtung **46** ist auch mit einer Bedienungspersonstation **50** gekoppelt, die einen Computermonitor **52**, eine Tastatur **54** sowie andere Eingabevorrichtungen **56** wie beispielsweise eine Maus umfaßt. Ferner umfaßt das CT-System **16** wie das MRI-System **14** im allgemeinen einen Drucker oder eine ähnliche Vorrichtung zur Ausgabe rekonstruierter Bilder basierend auf von der Abtasteinrichtung **42** gesammelten Daten.

Vorrichtungen anderer Modalität umfassen Schaltungen und Hardware, die zur Erfassung oder Erzeugung von Signalen gemäß ihrem speziellen Entwurf besonders konfiguriert sind. Insbesondere umfaßt das Ultraschallabbildungssystem **18** im allgemeinen eine Abtasteinrichtungs- und Datenverarbeitungseinheit **58** zur Übertragung von Ultraschallsignalen in ein Objekt von Interesse und zur Erfassung sich ergebender Signale, die zur Rekonstruktion eines verwendbaren Bilds verarbeitet werden. Das System umfaßt

eine Systemsteuereinrichtung **60**, die den Betrieb der Abtasteinrichtung **58** reguliert und erfaßte Signale zur Rekonstruktion des Bilds verarbeitet. Ferner umfaßt das System **18** ein Kommunikationsmodul **62** zur Übertragung von Dienstanforderungen, Nachrichten und Daten zwischen der Systemsteuereinrichtung **60** und der Dienstanlage **22**. Das System **18** umfaßt auch eine Bedienungspersonstation **64** einschließlich eines Monitors **66** sowie Eingabevorrichtungen wie beispielsweise einer Tastatur **68**.

Wenn mehr als ein medizinisches Diagnosesystem bei einer einzelnen Anlage oder einem einzelnen Ort bereitgestellt ist, wie es in dem Fall des MRI-Systems und des CT-Systems **14** und **16** in **Fig.** 1 angegeben ist, können diese mit einer Verwaltungsstation **70** gekoppelt sein wie beispielsweise bei einer Radiologieabteilung eines Krankenhauses oder einer Klinik. Die Verwaltungsstation kann mit Steuereinrichtungen für die verschiedenen Diagnosesysteme wie beispielsweise den Steuereinrichtungen **30** und **46** bei dem veranschaulichten Beispiel direkt verbunden sein. Das Verwaltungssystem kann eine Computer-Workstation oder einen Personal-Computer (WS) **72** umfassen, die mit den Systemsteuereinrichtungen in einer Intranetkonfiguration, in einer Konfiguration mit gemeinsamer Dateinutzung, in einer Client/Server-Anordnung oder in einer anderen geeigneten Anordnung gekoppelt sind. Die Verwaltungsstation **70** umfaßt typischerweise einen Monitor **74** zur Betrachtung von Systembetriebsparametern, zur Analyse der Systemnutzung und zum Austausch von Dienstanforderungen und Daten zwischen der entfernten Anlage **20** und der zentralen Dienstanlage **22**. Eingabevorrichtungen wie beispielsweise eine Standardcomputertastatur **76** und -maus **78** können zur Erleichterung bzw. Vereinfachung der Benutzerschnittstelle ebenfalls bereitgestellt sein. Es ist zu beachten, daß alternativ das Verwaltungssystem oder andere Diagnosesystemkomponenten dezentral, d. h. nicht direkt mit einem Diagnosesystem gekoppelt sein können. In derartigen Fällen können nichtsdestoweniger die beschriebene Dienstplattform und ein Teil der Dienstfunktionalität oder die gesamte Dienstfunktionalität bei dem Verwaltungssystem bereitgestellt sein. Ähnlich kann bei gewissen Anwendungen ein Diagnosesystem aus einem dezentralen oder vernetzten Bildarchivierungskommunikations- und -wiedergewinnungssystem oder einer Betrachtungsstation bestehen, die mit einem Teil der beschriebenen Funktionalität oder der gesamten beschriebenen Funktionalität versehen sind.

Die vorstehend angeführten Kommunikationsmodule sowie die Workstation **72** und die Außendiensteinheiten **24** können über ein Fernzugriffsnetz **80** mit der Dienstanlage **22** verbunden sein. Zu diesem Zweck kann jede geeignete Netzverbindung verwendet werden. Die bevorzugten Netzkonfigurationen umfassen sowohl proprietäre oder dedizierte Netze als auch offene Netze wie beispielsweise das Internet. Daten können zwischen den Diagnosesystemen, den Außendiensteinheiten **24** und der zentralen Dienstanlage **22** in jedem geeigneten Format ausgetauscht werden wie beispielweise gemäß dem Internetprotokoll bzw. Internet Protocol (IP), dem Übertragungssteuerprotokoll bzw. Transmission Control Protocol (TCP) oder anderen bekannten Protokollen. Ferner können gewisse Daten der Daten über Dokumentauszeichnungssprachen bzw. Markup-Sprachen wie beispielsweise die Hypertext-Dokumentauszeichnungssprache bzw. Hypertext Markup Language (HTML) oder andere Standardsprachen übertragen oder formatiert werden. Die bevorzugten Schnittstellenstrukturen und Kommunikationskomponenten sind nachstehend ausführlicher beschrieben.

In der Dienstanlage **22** werden Nachrichten, Dienstanforderungen und Daten von Kommunikationskomponenten empfangen, wie sie allgemein bei einem Bezugszeichen **82** angegeben sind. Die Komponenten **82** übertragen die Dienstdaten zu einem Dienstzentrumsverarbeitungssystem (PS), das allgemein bei einem Bezugszeichen **84** in **Fig.** 1 dargestellt ist. Das Verarbeitungssystem verwaltet den Empfang, die Handhabung und die Übertragung von Dienstdaten zu und von der Dienstanlage. Im allgemeinen kann das Verarbeitungssystem **84** einen Computer oder eine Vielzahl von Computern sowie dedizierte Hardware- oder Software-Server zur Verarbeitung der verschiedenen Dienstanforderungen und zum Empfangen und Senden der Dienstdaten umfassen, wie es nachstehend ausführlicher beschrieben ist. Die Dienstanlage **22** umfaßt auch eine Reihe von Bedienungsperson-Workstations (W) **86**, die mit Kundendiensttechnikern besetzt sein können, die sich mit den Dienstanforderungen befassen und einen Offline- und Online-Dienst für die Diagnosesysteme im Ansprechen auf die Dienstanforderungen bereitstellen. Ferner kann das Verarbeitungssystem **84** mit einem System von Datenbanken oder anderen Verarbeitungssystemen (DB) **88** bei der Dienstanlage **22** oder entfernt von der Dienstanlage **22** verbunden sein. Derartige Datenbanken und Verarbeitungssysteme können umfassende Datenbankinformationen über Betriebsparameter, Dienstverläufe usw. sowohl für spezielle teilnehmende Abtasteinrichtungen als auch für ausgedehnte Bestände von Diagnoseausstattung umfassen. Wie es nachstehend beschrieben ist, können derartige Datenbanken sowohl zum Vornehmen von Diensten bei speziellen Diagnosesystemen als auch zum Verfolgen eines derartigen Vornehmens von Diensten sowie zum Ableiten von Vergleichsdaten zur Verwendung bei einem Vornehmen von Diensten bei einem speziellen System oder einer Systemfamilie verwendet werden.

Fig. 2 zeigt ein Blockschaltbild, das die vorstehenden Systemkomponenten in einer funktionellen Ansicht veranschaulicht. Wie es in **Fig.** 2 gezeigt ist, können die entfernt angeordneten Außendiensteinheiten **24** und Diagnosesysteme **12** über eine Netzverbindung, wie sie allgemein bei dem Bezugszeichen **80** veranschaulicht ist, mit der zentralen Dienstanlage **22** verbunden sein. In jedem Diagnosesystem **12** ist eine einheitliche Dienstplattform **90** bereitgestellt. Die Plattform **90** umfaßt Hardware-, Firmware- und Softwarekomponenten, die zum Erzeugen und Übertragen von Dienstanforderungen und Dienstaufgabenlisten, zum Senden und Empfangen von Dienstdaten, zum Herstellen von Netzverbindungen und zum Verwalten von Finanz- oder Teilnehmervereinbarungen zwischen dem Diagnosesystem und der Dienstanlage eingerichtet sind. Die Plattform **90** ist vorzugsweise in der Systemsteuereinrichtung des Diagnosesystems integriert. Diese Plattformen stellen eine einheitliche grafische Benutzeroberfläche bei jedem Diagnosesystem bereit, die an verschiedene Systemmodalitäten angepaßt werden kann, um eine Interaktion von Klinikern und Radiologen mit den verschiedenen Diagnosesystemen für Dienstfunktionen zu ermöglichen. Die Plattformen ermöglichen es dem Abtasteinrichtungskonstrukteur, sich direkt mit den Steuerschaltungen der einzelnen Abtasteinrichtungen sowie mit Speichervorrichtungen bei den Abtasteinrichtungen in Verbindung zu setzen, um auf Bilddateien, Protokolldateien und ähnliche Dateien zuzugreifen, die zur Ausführung angeforderter oder abonnierter Dienste erforderlich sind. Wenn eine Verwaltungsstation **70** bereitgestellt ist, wird vorzugsweise eine ähnliche einheitliche Plattform auf die Verwaltungsstation geladen, um eine direkte Verbindung zwischen der Verwaltungsstation und der Dienstanlage zu ermöglichen. Zusätzlich zu der einheitlichen Dienstplattform **90** ist jedes Diagnosesystem vorzugsweise mit einem alternativen Kommunikationsmodul (F) **92** wie beispielsweise einem Faksimileübertragungsmodul zum Senden und

Empfangen von Faksimilenachrichten zwischen der entfernt angeordneten Abtasteinrichtung und der zentralen Dienstanlage versehen.

Zwischen den Diagnosesystemen und der Dienstanlage übertragene Nachrichten und Daten gehen durch eine in dem Verarbeitungssystem **84** enthaltene Sicherheitsbarriere oder "Firewall", wodurch ein nicht autorisierter Zugriff auf die Dienstanlage auf eine allgemein bekannte Art und Weise verhindert wird. Ein Modemgestell **96**, das eine Reihe von Modems (M) **98** umfaßt, empfängt die ankommenden Daten und sendet abgehende Daten durch einen Router **100**, der den Datenverkehr zwischen den Modems und dem Dienstzentrumsverarbeitungssystem **84** verwaltet.

Wie es vorstehend angeführt ist, empfängt und verarbeitet das Verarbeitungssystem **84** die Dienstanforderungen und Daten und ist mit zusätzlichen Dienstkomponenten sowohl bei der Dienstanlage als auch entfernt von der Anlage verbunden. Wie es in **Fig.** 2 gezeigt ist, sind Bedienungsperson-Workstations **86** sowie entfernte Datenbanken oder Computer **88** mit dem Verarbeitungssystem gekoppelt. Außerdem ist zumindest eine lokale Dienstdatenbank **102** zur Verifikation von Lizenz- und Vertragsvereinbarungen, zur Speicherung von Dienstaufzeichnungsdateien, Protokolldateien usw. bereitgestellt. Ferner sind ein Kommunikationsmodul oder mehrere Kommunikationsmodule **2104** zum Senden und Empfangen von Faksimileübertragungen zwischen der Dienstanlage und den Diagnosesystemen oder Außendiensteinheiten mit dem Verarbeitungssystem **84** verbunden.

Fig. 3 zeigt die verschiedenen funktionellen Komponenten, die die einheitliche Dienstplattform **90** in jedem Diagnosesystem **12** umfaßt. Diese einheitliche Dienstplattform kann bei dem bevorzugten Ausführungsbeispiel der Erfindung dazu verwendet werden, entfernten Systemen einen Zugriff auf Softwareanwendungen über ein Netz zu ermöglichen. Die einheitliche Plattform ist als in einem Web-Server **3118** gespeicherte Software resident. Der Web-Server **3118** ermöglicht einen Datenaustausch zwischen dem Diagnosesystem und der Dienstanlage und ermöglicht es, eine Reihe von Web-Seiten **3122** und **3124** über einen Web-Browser **3120** zu betrachten. Vorzugsweise unterstützen der Server **3118** und der Browser **3120** HTTP-Anwendungen, und der Browser unterstützt Java-Anwendungen. Bei der Haupt-Web-Seite **3122** handelt es sich vorzugsweise um eine Markup-Sprachen-Seite wie beispielsweise eine für den Systembenutzer auf einem Monitor bei dem Diagnosesystem angezeigte HTML-Seite. Auf die Haupt-Web-Seite **3122** kann vorzugsweise von einer normalen Betriebsseite aus zugegriffen werden, bei der der Benutzer Untersuchungsanforderungen konfiguriert, die Ergebnisse von Untersuchungen betrachtet usw., wie beispielsweise über ein Symbol am Bildschirm. Durch die Haupt-Web-Seite **3122** kann auf eine Reihe von zusätzlichen Web-Seiten (WP) **3124** zugegriffen werden. Derartige Web-Seiten ermöglichen es, Dienstanforderungen und Anforderungen zum Zugriff auf Softwareanwendungen zu erzeugen sowie zu der zentralen Dienstanlage zu übertragen, und ermöglichen den Austausch von anderen Nachrichten, Berichten, Software, Protokollen usw., wie es nachstehend ausführlicher beschrieben ist. Der Web-Server **3118** kommuniziert über ein Modem **3130** mit einem Netz. Ein Konnektivitätsdienstmodul **3126** sorgt für die Verbindung mit dem Web-Server **3118**. Ein Punkt-zu-Punkt-Protokoll-Modul bzw. Point-to-Point-Protokoll-Modul (PPP-Modul) **3128** ist zur Übertragung von Internet-Protocol-Paketen (IP-Paketen) über Fernkommunikationsverbindungen ebenfalls bereitgestellt. Wie es von Fachleuten zu erkennen ist, können zur Ermöglichung eines Datenaustauschs über ein Netz verschiedene andere Netzprotokolle und Komponenten verwendet werden.

Ein Gemeinschaftsverwaltungssystem kann in dem in **Fig.** 2 gezeigten Dienstzentrumsverarbeitungssystem enthalten sein. Alternativ kann es sich bei dem offenbarten Gemeinschaftsverwaltungssystem um ein dezentrales System handeln. Die bevorzugten Ausführungsbeispiele des Gemeinschaftsverwaltungssystems sind in **Fig.** 4 und 5 allgemein gezeigt. Bei jedem Ausführungsbeispiel umfaßt das System eine Vielzahl von verteilten Web-Servern **110**, die über eine Firewall **138** mit zumindest einem Richtlinien-Server **114** kommunizieren. Jeder Web-Server **110** ist dazu programmiert, einen Zugriff auf eine Softwareanwendung oder mehrere Softwareanwendungen bereitzustellen, die sich bei dem Web-Server selbst befinden können oder bei jeweiligen Anwendungs-Servern befinden können, die mit dem Web-Server **110** verbunden sind. Die Web-Server kommunizieren mittels Netzen mit entfernten Systemen. Die Softwareanwendungen können in dem Sinn geschützt sein, daß sie eine Sicherheitsfreigabe zum Zugriff erfordern, oder in dem Sinn frei sein, daß sie für jeden öffentlich verfügbar sind, der mit dem Netz verbunden ist. Wie es nachstehend ausführlicher erläutert ist, fallen die geschützten Softwareanwendungen bei dem bevorzugten Gemeinschaftsverwaltungsschema in zwei Kategorien: (**1**) diejenigen, die zum Zugriff eine Sicherheitsfreigabe mit einem Faktor (z. B. einem Kennwort) erfordern; und (**2**) diejenigen, die eine Sicherheitsfreigabe mit zwei Faktoren (z. B. einem Kennwort und einer zufällig erzeugten Sicherheitscodezahl) erfordern. **Fig.** 4 soll einen Teil eines Gemeinschaftsverwaltungssystems zeigen, das ein Sicherheitsschema mit einem Faktor verwendet, während **Fig.** 5 einen Teil eines Gemeinschaftsverwaltungssystems zeigen soll, das ein Sicherheitsschema mit zwei Faktoren verwendet. **Fig.** 5 unterscheidet sich darin von **Fig.** 4, daß sie zusätzlich einen Sicherheits-Server **126** aufweist, der mit dem Richtlinien-Server **114** kommuniziert und der dazu programmiert ist, den zweiten Faktor des Sicherheitstests mit zwei Faktoren zu beglaubigen, wie es nachstehend ausführlicher beschrieben ist.

Die auf die Web-Server zugreifenden entfernten Systeme können medizinische Diagnosesysteme einschließlich Abbildungs- und Überwachungssystemen umfassen. Beispielsweise zeigt **Fig.** 4 einen Browser **104** einer Abbildungsabtasteinrichtung und einen Browser **106** eines Krankenhausabteilungs-Personal-Computers, die jeweils über ein Fernzugriffsnetz **80** auf einen Web-Server **110** zugreifen können, sowie einen Browser **108**, der über das Internet **81** auf einen Web-Server **110** zugreifen kann. Jeder Web-Server **110** ist mit einem Agenturmodul **112** zum Abfangen von Anforderungen zum Zugriff, zur Bestimmung, ob die angeforderte Software offen oder geschützt ist, und zur Kontaktierung eines Richtlinien-Servers **114**, falls die Software geschützt ist, programmiert. Das Agenturmodul **112** stellt eine Schnittstelle zur Kommunikation zwischen dem Web-Server **110** und dem Richtlinien-Server **114** bereit.

Das bevorzugte Ausführungsbeispiel umfaßt ferner eine Gemeinschaftsverwaltungsdatenbank **116**. Im allgemeinen enthält die Datenbank **116** Daten eines entfernten Standorts, Vertrags- oder Teilnahmedaten, Kontakt- oder Benutzerdaten und Geschäftsregeln (d. h. Gemeinschaftsdefinitionen). Der Ausdruck "Gemeinschaft", wie er dabei verwendet ist, bezieht sich auf eine Gruppe von Benutzern eines entfernten Systems mit einem speziellen Satz von Zugriffsrechten. Der Ausdruck "Softwareanwendung", wie er dabei verwendet ist, soll Software jeder Art einschließlich Anwendungsprogrammierung, Konfigurationsdateien, Protokollen, Datendateien, Arbeitslisten, Dienstberichten, Diensthilfseinrichtungen, Systemverläufen, Systemleistungsdaten, proprietären Informationen über bei entfernten medizinischen Dia-

gnosesystemen verwendete Software, Reparaturverfahren, Geschäftsaufzeichnungen usw., jedoch nicht darauf beschränkt, umfassen. Die in der Gemeinschaftsverwaltungsdatenbank **116** gespeicherten Geschäftsregeln stellen die Kriterien zur Bestimmung der Softwareanwendungen, für die ein Mitglied einer speziellen Gemeinschaft über Zugriffsrechte verfügt, bereit. Die Kontakt- oder Benutzerdaten in der Datenbank **116** umfassen Benutzernamen, Kennwörter, Sicherheitscodes, Keimzahlen, Zufallszahlenerzeugungsaktivierungszeiten, Benutzerstellenstatus oder -titel und andere Informationen. Die Vertragsdaten umfassen Informationen über die Softwareanwendungen, für die teilnehmende Parteien entsprechend vorhandenen Verträgen zwischen entfernten Anlagen und der zentralen Dienstanlage zum Zugriff berechtigt sind. Die Standortdaten umfassen Informationen, die die entfernten Standorte und die an den Standorten verwendete Ausstattung identifizieren, einschließlich Seriennummern der Diagnose- und Abbildungsgeräte.

Das bevorzugte Ausführungsbeispiel der Erfindung umfaßt Web-Server **110** zur Bereitstellung eines selektiven Zugriffs auf Softwareanwendungen mit einer hohen Stufe des Schutzes, d. h. auf Softwareanwendungen, die eine Sicherheitsfreigabe mit zwei Faktoren erfordern. Softwareanwendungen mit dieser hohen Sicherheitsstufe umfassen dienstbezogene Software, die von einem Außendiensttechniker zur Reparatur, zum Vornehmen von Diensten, zur Aktualisierung oder zur Wartung bei einem entfernten Diagnosesystem verwendet wird, wie beispielsweise in **Fig.** 5 gezeigte Diensthilfseinrichtungen **128** und Dienstaufzeichnungen **130**. Beispielsweise kann einem von der zentralen Dienstanlage beschäftigten Außendiensttechniker eine Sicherheitsfreigabe mit zwei Faktoren erteilt werden, die einen Fernzugriff z. B. über den Browser **104** einer entfernten Abbildungsabtasteinrichtung und über ein Netz auf Softwareanwendungen ermöglicht, die zum Vornehmen von Diensten bei der Abbildungsabtasteinrichtung benötigt werden. Bei dem ersten Faktor handelt es sich um den gleichen Faktor, der bei der Sicherheitsfreigabe mit einem Faktor verwendet wird, und er wird durch den Richtlinien-Server **114** beglaubigt. Gemäß dem in **Fig.** 5 gezeigten bevorzugten Ausführungsbeispiel ist ein Sicherheits-Server **126** dazu programmiert, den zweiten Faktor der Sicherheitsfreigabe mit zwei Faktoren unter der Verwaltung des Richtlinien-Servers **114** zu beglaubigen.

Das bevorzugte Verfahren zur Verarbeitung von Sicherheitsfreigaben ist in **Fig.** 6 gezeigt. Jedes entfernte System ist mit einer Benutzerschnittstelle der in **Fig.** 3 gezeigten Art zum Zugriff auf einen Web-Server **110** über ein Netz **80** wie beispielsweise ein Intranet programmiert. Bei einer der Web-Seiten **3124** kann es sich um eine Anwendungs-Web-Seite handeln, die eine Vielzahl von virtuellen Anwendungsauswahlknöpfen zur Auswahl einer Softwareanwendung aus einer Vielzahl von dienstbezogenen (offenen oder geschützten) Softwareanwendungen, auf die aus der Entfernung zugegriffen werden kann und die sich bei den Web-Servern **110** befinden, anzeigt. Aus Gründen der Erörterung wird angenommen, daß die sich bei in **Fig.** 4 gezeigten Web-Servern **110** befindenden geschützten Softwareanwendungen eine Sicherheitsfreigabe mit einem Faktor zum Zugriff erfordern. Demgegenüber erfordert zumindest eine der sich bei einem in **Fig.** 5 gezeigten Web-Server **110** befindenden geschützten Softwareanwendungen eine Sicherheitsfreigabe mit zwei Faktoren zum Zugriff, wodurch das Vorhandensein des Sicherheits-Servers **126** erforderlich ist. Es ist ferner selbstverständlich, daß einige Softwareanwendungen offen und nicht geschützt sein können. Die Erfindung ist jedoch hauptsächlich auf die Handhabung eines Fernzugriffs auf geschützte Softwareanwendungen gerichtet.

Im Ansprechen auf eine Auswahl einer geschützten Softwareanwendung auf dem Web-Browser-Bildschirm durch den Systembenutzer überträgt der Web-Server **3118** bei dem entfernten System über in **Fig.** 3 gezeigte Blöcke **3126**, **3128** und **3130** eine Anforderung zum Zugriff auf die ausgewählte Softwareanwendung zu dem Netz (Schritt **160** in **Fig.** 6). Vorzugsweise ist die URL-Adresse des Web-Servers **110**, bei dem sich die ausgewählte Softwareanwendung befindet, fest in das entfernte System codiert, wobei die URL-Adresse vor der Verbindung mit dem Netz automatisch der Anforderung zum Zugriff beigefügt wird.

Die Anforderung zum Zugriff von dem entfernten System zu dem adressierten Web-Server **110** wird unmittelbar durch das Agenturmodul **112** des Web-Servers abgefangen, das zuerst bestimmt, ob sich die Anforderung zum Zugriff auf eine offene oder eine geschützte Softwareanwendung bezieht. Wenn die Softwareanwendung offen ist, d. h. ohne eine Sicherheitsfreigabe verfügbar, dann weist das Agenturmodul den Web-Server so an, und die Anwendung wird dem entfernten System zugestellt. **Fig.** 6 stellt den Prozeß zur Genehmigung von Anforderungen zum Zugriff auf geschützte Software dar.

Falls die angeforderte Softwareanwendung eine Sicherheitsfreigabe erfordert, bestimmt das Agenturmodul daraufhin, ob der anfordernde Benutzer eines entfernten Systems bereits beglaubigt wurde (Schritt **162** in **Fig.** 6), d. h. sich bereits angemeldet hat. Wenn der Benutzer bereits angemeldet ist, dann wird der Beglaubigungsschritt übersprungen, und der Richtlinien-Server bestimmt unmittelbar, ob der angeforderte Zugriff genehmigt ist (Schritt **168**). Falls der anfordernde Benutzer des entfernten Systems nicht bereits angemeldet ist, lädt der adressierte Web-Server ein Fenster zu dem entfernten Web-Browser herunter, das Felder zur Eingabe des Namens, des Kennworts und des Sicherheitscodes des Benutzers aufweist. Der Benutzer des entfernten Systems gibt daraufhin die Benutzeridentifizierungsinformationen ein, die von dem Richtlinien-Server benötigt werden (Schritt **164**). In dem Fall eines Benutzers mit einer Sicherheitsfreigabe mit einem Faktor gibt der Benutzer vorzugsweise einen Benutzernamen und ein Kennwort ein; in dem Fall eines Benutzers mit einer Sicherheitsfreigabe mit zwei Faktoren gibt der Benutzer vorzugsweise einen Benutzernamen, ein Kennwort und einen von einer im Besitz des Benutzers befindlichen Zufallszahlenerzeugungseinrichtung erzeugten Sicherheitscode ein. Der Web-Server **3118** bei dem entfernten System (siehe **Fig.** 3) überträgt daraufhin die eingegebenen Benutzerinformationen an den Web-Server **110** (siehe **Fig.** 4 und 5) adressiert, bei dem sich die angeforderte Softwareanwendung befindet, auf das Netz. Die übertragenen Benutzerinformationen werden von dem Agenturmodul **112** abgefangen und zusammen mit einem die geschützte Softwareanwendung, auf die sich die Anforderung zum Zugriff bezieht, identifizierenden Code zu dem Richtlinien-Server **114** weitergeleitet.

Im dem Fall der Sicherheitsfreigaben mit einem Faktor beglaubigt der Richtlinien-Server das Kennwort (Schritt **166**) unter Bezugnahme auf eine Benutzerdatenbank **124**, die einen Teil der Gemeinschaftsverwaltungsdatenbank bildet. Bei dem einfachsten Ausführungsbeispiel speichert die Benutzerdatenbank ein Kennwort in Verbindung mit jedem Benutzernamen, und der Richtlinien-Server gewinnt lediglich das Kennwort wieder und vergleicht es mit dem von dem Agenturmodul, bei dem sich die angeforderte Software befindet, empfangenen Kennwort. Falls das Kennwort nicht glaubwürdig ist, überträgt der adressierte Web-Server eine Fehlermeldung zu dem entfernten System. Wenn der Benutzercode glaubwürdig ist, dann muß der Richtlinien-Server

als nächstes bestimmen, ob der angeforderte Zugriff genehmigt ist (Schritt **168**). In dem Fall der Sicherheitsfreigaben mit zwei Faktoren beglaubigt der Richtlinien-Server ein Kennwort, während er die Beglaubigung eines zugeordneten Sicherheitscodes an den Sicherheits-Server delegiert (Schritt **165**). Wenn das Kennwort und der Sicherheitscode glaubwürdig sind, dann geht der Richtlinien-Server zu dem Genehmigungsstadium (Schritt **168**) über.

Gemäß dem bevorzugten Ausführungsbeispiel der Erfindung ist der Richtlinien-Server dazu programmiert, zu bestimmen, ob der Benutzer eines entfernten Systems zum Zugriff auf die geschützte Softwareanwendung befugt ist, indem er die nachstehenden Schritte ausführt: Wiedergewinnen von Genehmigungskriterien (d. h. Geschäftsregeln oder Gemeinschaftsdefinitionen **118**) für die geschützte Softwareanwendung aus der Gemeinschaftsverwaltungsdatenbank; Wiedergewinnen von Informationen für eine Variable oder mehrere Variablen (d. h. Benutzer-, Standort-, System- und Vertragsinformationen) aus der Gemeinschaftsverwaltungsdatenbank; und Bestimmen, ob die Variablen die Genehmigungskriterien erfüllen. Der Richtlinien-Server **114** liest alle sachdienlichen Daten für den identifizierten Benutzer des entfernten Systems aus der Gemeinschaftsverwaltungsdatenbank aus und speichert die wiedergewonnenen Daten in einem internen Anmeldungshilfsspeicher bzw. Anmeldungscache. Basierend auf den während des Genehmigungsschritts **168** wiedergewonnenen Kriterien und Variablendaten bestimmt der Richtlinien-Server **114**, ob der anfordernde Benutzer des entfernten Systems über Zugriffsrechte für die angeforderte Softwareanwendung verfügt (Schritt **170**).

Wenn der anfordernde Benutzer eines entfernten Systems zum Zugriff auf die angeforderte geschützte Softwareanwendung befugt ist, dann gibt der Richtlinien-Server eine Anweisung zu dem Agenturmodul aus, bei dem sich die geschützte Software befindet, um den Zugriff zu ermöglichen. Der zugeordnete Web-Server lädt daraufhin die geschützte Softwareanwendung zu dem entfernten System herunter, bei dem der anfordernde Benutzer angemeldet ist (Schritt **178**). Als Folge des Herunterladens zeigt der Web-Server **3118** (siehe **Fig.** 3) bei dem entfernten System die Eröffnungs-Web-Seite der heruntergeladenen Softwareanwendung auf dem Web-Browser **3120** an.

Optional umfaßt der in **Fig.** 6 gezeigte Algorithmus einen Schritt **174** der Bestimmung, ob die Softwareanwendung vor der Zustellung personalisiert werden soll, z. B. durch eine Einfügung einer Willkommensnachricht, in der der Benutzer mit seinem Namen angeredet wird. Personalisierungsdienste werden von dem Web-Server **110** (siehe **Fig.** 4) in einem Schritt **176** ausgeführt. Daraufhin wird die personalisierte Anwendung in dem Schritt **178** dem entfernten Standort zugestellt.

Der Richtlinien-Server ist ferner dazu programmiert, das Agenturmodul des Web-Servers, bei dem sich die angeforderte Software befindet, zur Ablehnung des Zugriffs anzuweisen, falls der Benutzer eines entfernten Systems Mitglied einer Gemeinschaft ist, die nicht zum Zugriff auf die geschützte Software befugt ist. Optional ist der Web-Server, bei dem sich die geschützte Software befindet, dazu programmiert, dem entfernten System im Ansprechen auf eine Ablehnung des Zugriffs durch den Richtlinien-Server eine alle Softwareanwendungen, für die der anfordernde Benutzer des entfernten Systems über Zugriffsrechte verfügt, identifizierende Liste zuzustellen (Schritt **172**).

Gemäß einem bevorzugten Ausführungsbeispiel wird der Schritt **162** (siehe **Fig.** 6) der Bestimmung, daß der Benutzercode bereits beglaubigt ist, d. h. daß der Benutzer eines entfernten Systems sich bereits erfolgreich angemeldet hat, wie folgt ausgeführt. Der Web-Browser bei jedem entfernten System und das Agenturmodul bei jedem Anwendungs-Web-Server umfassen einen Anmeldungscache zur Speicherung der Benutzereingaben (z. B. Benutzername, Kennwort und Sicherheitscode) und einer zugeordneten Glaubwürdigkeitskennzeichnung, die nach einer Beglaubigung durch den Richtlinien-Server erzeugt wird. Die Operationssequenz stellt sich wie folgt dar. (1) der Benutzer des entfernten Systems überträgt eine Anforderung zum Zugriff zu einem ersten Web-Server. (2) Der erste Web-Server lädt daraufhin eine Web-Seite herunter, die den Benutzer des entfernten Systems zur Anmeldung auffordert. (3) Der Benutzer des entfernten Systems gibt daraufhin einen Benutzernamen und ein Kennwort (Sicherheitsfreigabe mit einem Faktor) oder einen Benutzernamen, ein Kennwort und einen Sicherheitscode (Sicherheitsfreigabe mit zwei Faktoren) über die Benutzerschnittstelle ein und überträgt die eingegebenen Daten zu dem ersten Web-Server, wobei die Benutzerinformationen automatisch in einem Anmeldungscache des Web-Browsers gespeichert werden. (4) Der Agent des ersten Web-Servers fängt die eingegebenen Benutzerinformationen ab und überträgt sie zu dem Richtlinien-Server. (5) Falls die Benutzerinformationen glaubwürdig sind, fügt der Richtlinien-Server eine Glaubwürdigkeitskennzeichnung bei, speichert die Benutzerinformationen und die Glaubwürdigkeitskennzeichnung in seinem Anmeldungscache und überträgt die gleichen Daten zurück zu dem Agenten des ersten Web-Servers. (6) Die gleichen Daten werden daraufhin in dem Anmeldungscache des Agenturmoduls gespeichert und zurück zu dem entfernten System übertragen, wobei die Benutzerinformationen und die Glaubwürdigkeitskennzeichnung in dem Anmeldungscache des Web-Browsers gespeichert werden. (7) Wenn der Benutzer des entfernten Systems nachfolgend eine Anforderung zum Zugriff auf einen zweiten Web-Server überträgt, werden die in dem Anmeldungscache des Web-Browsers gespeicherten Benutzerinformationen und die in dem Anmeldungscache des Web-Browsers gespeicherte Glaubwürdigkeitskennzeichnung automatisch zu dem zweiten Web-Server übertragen. (8) Der Agent des zweiten Web-Servers gibt daraufhin die empfangenen Benutzerinformationen und die empfangene Glaubwürdigkeitskennzeichnung an den Richtlinien-Server weiter. (9) Wenn die von dem zweiten Web-Server übertragenen Benutzerinformationen und die von dem zweiten Web-Server übertragene Glaubwürdigkeitskennzeichnung zu den in dem Anmeldungscache des Richtlinienservers gespeicherten Benutzerinformationen und der in dem Anmeldungscache des Richtlinien-Servers gespeicherten Glaubwürdigkeitskennzeichnung passen, dann überträgt der Richtlinien-Server ein Signal zu dem zweiten Web-Server; das angibt, daß der Benutzercode glaubwürdig ist. Somit weiß der zweite Web-Server, daß er den Schritt des Herunterladens der Anmeldungs-Web-Seite zu dem entfernten System überspringen kann. Diese Operationen bewirken, daß es für einen mehrere Softwareanwendungen anfordernden Benutzer eines entfernten Systems nicht erforderlich ist, sich mehrmals anzumelden. Statt dessen reicht eine einzelne Anmeldung aus, ganz gleich wie viele Anforderungen zum Zugriff auf Softwareanwendungen von einem angemeldeten entfernten Benutzer veranlaßt werden.

Gemäß einer weiteren Ausgestaltung der Erfindung erfordert ein Zugriff auf Softwareanwendungen mit einer hohen Stufe des Schutzes eine Sicherheitsfreigabe mit zwei Faktoren. Wie es vorstehend beschrieben ist, handelt es sich bei dem ersten Faktor um ein mit einem Benutzernamen verbundenes geheimes Kennwort. Bei dem zweiten Faktor handelt es sich um eine zufällig erzeugte Zahl, die ein Benutzer eines entfernten Systems von einer tragbaren Vorrichtung wie beispielsweise einer Uhrtasche (fob) liest, die er/sie

trägt. Die tragbare Vorrichtung enthält eine Zufallszahlenerzeugungseinrichtung zur fortwährenden Erzeugung von Zahlen gemäß einem gespeicherten Zufallszahlenerzeugungsalgorithmus und einen Bildschirm, der den derzeitigen Wert in der Sequenz von zufällig erzeugten Zahlen anzeigt. Die Zufallszahlenerzeugungseinrichtung wird durch die zentrale Dienstanlage mit einer Keimzahl beginnend aktiviert, die von dem zentralen Dienstleister in die tragbare Vorrichtung eingegeben wird. Die Zeit der Zufallszahlenerzeugungsaktivierung wird daraufhin zusammen mit dem Benutzernamen, dem Kennwort, der Keimzahl und anderen Benutzerinformationen in der Benutzerdatenbank gespeichert.

Basierend auf dem Vorhandensein eines Sicherheitscodes in den über das Agenturmodul **112** (siehe **Fig. 5**) von dem Benutzer eines entfernten Systems empfangenen Benutzerinformationen erkennt der Richtlinien-Server **114**, daß eine Sicherheitsfreigabe mit zwei Faktoren ausgeführt werden muß. Basierend auf dem Benutzernamen gewinnt der Richtlinien-Server **114** daraufhin die Benutzerinformationen für den Benutzer aus der Gemeinschaftsverwaltungsdatenbank **116** wieder. Der Richtlinien-Server **114** vergleicht das eingegebene Kennwort mit dem aus der Datenbank wiedergewonnenen Kennwort. Falls sie zusammenpassen, überträgt der Richtlinien-Server daraufhin den von dem Benutzer eingegebenen Sicherheitscode sowie die aus der Datenbank wiedergewonnene Keimzahl und Aktivierungszeit für die Zufallszahlenerzeugung zu dem Sicherheits-Server **126**. Basierend auf der von dem Richtlinien-Server empfangenen Aktivierungszeit und Keimzahl sowie dem in dem Sicherheits-Server gespeicherten Zufallszahlenerzeugungsalgorithmus (bei dem es sich um den gleichen Algorithmus wie den in der von dem Benutzer getragenen Zufallszahlenerzeugungseinrichtung enthaltenen Algorithmus handelt) erzeugt der Sicherheits-Server eine Zufallszahl zur Verwendung als Bezugssicherheitscode. Der von dem Benutzer eingegebene Sicherheitscode wird beglaubigt, falls er in einem vorbestimmten Bereich des Bezugssicherheitscodes liegt. Der Sicherheits-Server benachrichtigt daraufhin den Richtlinien-Server von den Ergebnissen des Vergleichs. Falls der eingegebene Sicherheitscode glaubwürdig ist, geht der Richtlinien-Server daraufhin zu dem Genehmigungsschritt über. Wenn der Sicherheitscode nicht glaubwürdig ist, dann weist der Richtlinien-Server das relevante Agenturmodul zur Ablehnung des Zugriffs auf die angeforderte Softwareanwendung an. Das Agenturmodul kann daraufhin den Benutzer des entfernten Systems auffordern, erneut zu versuchen, sich anzumelden.

Fig. 7 veranschaulicht beispielhafte funktionelle Komponenten für eine die Erfindung enthaltende Dienstanlage **22**. Wie es vorstehend angegeben ist, umfaßt die Dienstanlage **22** ein Modemgestell **96** mit einer Vielzahl von Modems **98**, die mit einem Router **100** zur Koordination von Datenübertragungen mit der Dienstanlage gekoppelt sind. Ein sogenannter HTTP-Dienst-Server **94** des "kundenbezogenen Bereichs" ("front office") empfängt und lenkt ankommende und abgehende Übertragungen mit der Anlage. Vorzugsweise sind die Anwendungs-Web-Server ebenfalls vor der Firewall **138** angeordnet. In **Fig. 7** ist lediglich ein Anwendungs-Web-Server **110** mit einem Agenturmodul **112** gezeigt. Die Server **94** und **110** sind mit den anderen Komponenten der Anlage durch die Firewall **138** für die Systemsicherheit gekoppelt. Bedienungsperson-Workstations **86** sind mit der Anschlußverwaltungseinrichtung zur Handhabung von Dienstanforderungen und Übertragung von Nachrichten und Berichten im Ansprechen auf derartige Anforderungen gekoppelt. Eine automatisierte Diensteinheit **136** kann ebenfalls in der Dienstanlage enthalten sein, um automatisch auf gewisse Dienstanforderungen anzusprechen, teilnehmende Diagnosesysteme nach Betriebsparameterdaten abzutasten usw.. Bei einem bevorzugten Ausführungsbeispiel kann die automatisierte Diensteinheit **136** unabhängig von oder in Verbindung mit den interaktiven Dienstkomponenten arbeiten, die das Verarbeitungssystem **84** umfaßt. Es ist zu beachten, daß andere Netz- oder Kommunikationsschemata bereitgestellt sein können, um es der Dienstanlage zu ermöglichen, Daten und Nachrichten mit Diagnosesystemen und zentralen Diensteinheiten wie beispielsweise Systemen einschließlich äußerer Internet-Dienstleister bzw. Internet-Serviceprovider und virtueller privater Netze zu übertragen und auszutauschen.

Hinter der Firewall **138** koordiniert ein sogenannter HTTP-Anwendungs-Server **140** der "technischen Abwicklung" ("back office") die Handhabung von Dienstanforderungen, Nachrichtenübermittlung, Berichterstattung, Softwareübertragungen usw.. Andere Server können mit dem HTTP-Anwendungs-Server **140** gekoppelt sein wie beispielsweise Dienstanalyse-Server **142**, die zur Befassung mit spezifischen Arten von Dienstanforderungen konfiguriert sind. Bei dem in **Fig. 7** gezeigten Ausführungsbeispiel umfaßt das Verarbeitungssystem **84** auch einen Richtlinien-Server **114**, einen Sicherheits-Server **126** und einen Lizenz-Server **144**. Der Richtlinien-Server und der Lizenz-Server sind beide mit einer Richtlinien-/Lizenzdatenbank **146** gekoppelt, die die vorstehend angeführte Gemeinschaftsverwaltungsdatenbank sowie eine Lizenzdatenbank umfaßt. Ein Lizenzmodul **144** führt die Funktionen des Speicherns, Aktualisierens und Verifizierens des Status von Diagnosesystemdienstteilnahmen und -verträgen aus. Alternativ kann der Lizenz-Server **144** außerhalb der Firewall **138** angeordnet sein, um den Teilnahmestatus vor dem Zugang zu der Dienstanlage zu verifizieren. Der Richtlinien-Server **114** führt die vorstehend unter Bezugnahme auf **Fig. 4** bis 6 beschriebenen Funktionen aus. Der Lizenz-Server **144** erzeugt Lizenzen, installiert die erzeugten Lizenzen über das Netz **80** auf den entfernten Systemen **12** und protokolliert die Lizenzen in die Richtlinien-/Lizenzdatenbank **146**. Der Lizenz-Server **144** weist ferner die Fähigkeit zur Entfernung oder Beendung einer installierten Lizenz von einem entfernten System über das Netz auf.

Die Handhabung von Dienstanforderungen, Nachrichtenübermittlung und Berichterstattung wird durch ein Schedulermodul **148** koordiniert, das mit dem HTTP-Server **140** gekoppelt ist. Das Schedulermodul **148** koordiniert Aktivitäten anderer Server, die das Verarbeitungssystem umfaßt, wie beispielsweise eines Bericht-Servers **150**, eines Nachrichten-Servers **152** und eines Softwareherunterlade-Servers **154**. Wie es von Fachleuten zu erkennen ist, sind die Server **150**, **152** und **154** mit (nicht gezeigten) Speichervorrichtungen zur Speicherung von Daten wie beispielsweise Aufgabenlisten, Adressen, Protokolldateien, Nachrichten- und Berichtdateien, Anwendungssoftware usw. gekoppelt. Wie es in **Fig. 7** veranschaulicht ist, ist insbesondere der Software-Server **154** über einen Datenkanal oder mehrere Datenkanäle mit einer Speichervorrichtung **156** zum Enthalten übertragbarer Softwarepakete gekoppelt, die direkt zu den Diagnosesystemen übertragen werden können, auf die von den Diagnosesystemen zugegriffen werden kann oder die auf der Grundlage einer Bezahlung pro Verwendung oder eines Kaufs geliefert werden können. Der Nachrichten- und der Bericht-Server **152** und **150** sind ferner zusammen mit dem Kommunikationsmodul **2104** mit einem Zustellungshandhabungsmodul (DEL) **158** gekoppelt, das zum Empfangen abgehender Nachrichten, zur Sicherstellung einer richtigen Konnektivität mit Diagnosesystemen und zur Koordination der Übertragung von Nachrichten zu den Diagnosesystemen

und der Übertragung von Nachrichten und Aufgabenlisten zu entfernt befindlichen Außendiensttechnikern über das Netz konfiguriert ist.

Bei einem bevorzugten Ausführungsbeispiel können die vorstehenden funktionellen Schaltungen als Hardware, Firmware oder Software auf jeder geeigneten Computerplattform konfiguriert sein. Beispielsweise können die funktionellen Schaltungen der Diagnosesysteme als geeigneter Code in einem Personal-Computer oder einer Workstation programmiert sein, die entweder vollständig in der Systemabtasteinrichtung enthalten sind oder zu der Systemabtasteinrichtung hinzugefügt sind. Die funktionellen Schaltungen der Dienstanlage können zusätzliche Personal-Computer oder Workstations zusätzlich zu einem Großrechner, in dem einer oder mehrere der Server, der Scheduler usw. konfiguriert sind, umfassen. Schließlich können die Außendiensteinheiten Personal-Computer oder Laptop-Computer von jeder geeigneten Prozessorplattform umfassen. Es ist ferner zu beachten, daß die vorstehenden funktionellen Schaltungen zur Ausführung der beschriebenen Funktionen auf vielfältige Art und Weise angepaßt sein können. Allgemein ermöglichen die funktionellen Schaltungen den Austausch von Dienstdaten zwischen den Diagnosesystemen und einer zentralen Dienstanlage, der vorzugsweise auf eine interaktive Art und Weise realisiert ist, um regelmäßige Aktualisierungen für die Diagnosesysteme hinsichtlich Dienstaktivitäten bereitzustellen.

Obwohl das offenbarte bevorzugte Ausführungsbeispiel Modems zur Ermöglichung einer Kommunikation mit einem Fernzugriffsnetz verwendet, sollte erkannt werden, daß keine Modems zur Verwirklichung der Erfindung erforderlich sind. Insbesondere können das Internet oder private Netze verwendet werden.

Während die Erfindung unter Bezugnahme auf bevorzugte Ausführungsbeispiele beschrieben ist, ist es für Fachleute offensichtlich, daß verschiedene Änderungen ausgeführt werden können und daß Elemente davon durch Äquivalente ersetzt werden können, ohne den Bereich der Erfindung zu verlassen. Darüber hinaus können viele Modifikationen ausgeführt werden, um eine spezielle Situation an die Lehre der Erfindung anzupassen, ohne ihren wesentlichen Bereich zu verlassen. Daher soll die Erfindung nicht auf das offenbarte, als die beste Form zur Ausführung der Erfindung betrachtete spezielle Ausführungsbeispiel beschränkt sein, sondern die Erfindung soll alle Ausführungsbeispiele umfassen, die in den Schutzbereich der beigefügten Patentansprüche fallen.

Der Ausdruck "Softwareanwendung", wie er in den Patentansprüchen verwendet ist, soll Software jeder Art einschließlich Anwendungsprogrammierung, Konfigurationsdateien, Protokollen, Datendateien, Arbeitslisten, Dienstberichten, Systemverläufen, Diensthilfseinrichtungen, Systemleistungsdaten, proprietären Dokumenten, Reparaturverfahren, Geschäftsaufzeichnungen usw., jedoch nicht darauf beschränkt, umfassen.

Die Erfindung stellt ein Verfahren und ein System zur Zustellung geschützter Softwareanwendungen von einer zentralen Dienstanlage (**22**) zu entfernten Systemen (**12**) bereit, wobei die Zustellung auf der Grundlage der Gemeinschaftsmitgliedschaft des Benutzers eines entfernten Systems verwaltet wird. Es werden Geschäftsregeln (**118**) verwendet, um zu bestimmen, ob ein spezieller beglaubigter Benutzer, der einen Zugriff auf eine geschützte Softwareanwendung von einem speziellen entfernten Standort anstrebt, berechtigt werden soll. Eine Vielzahl von Web-Servern (**110**) ist dazu programmiert, einen selektiven Zugriff auf eine residente Softwareanwendung oder mehrere residente Softwareanwendungen durch Benutzer eines entfernten Systems über ein Netz (**80**) zu ermöglichen. Der Zugriff wird durch einen zentralen Richtlinien-Server (**114**) basierend auf Benutzer- und Systeminformationen sowie Gemeinschaftsdefinitionen, die in einer Datenbank (**116**) gespeichert sind, verwaltet. Der Richtlinien-Server kommuniziert mit jedem Web-Server über ein in dem Web-Server enthaltenes Agenturmodul (**112**). Das Agenturmodul fängt Anforderungen zum Zugriff von Benutzern eines entfernten Systems ab und verbindet sich daraufhin mit dem Richtlinien-Server. Der Richtlinien-Server beglaubigt Kennwörter, während er die Beglaubigung zugeordneter Sicherheitscodes an einen Sicherheits-Server (**126**) übergibt. Falls das Kennwort und der Sicherheitscode beglaubigt werden, wendet der Richtlinien-Server daraufhin die Geschäftsregeln an, um zu bestimmen, ob der anfordernde Benutzer eines entfernten Systems dazu befugt ist, auf die angeforderte geschützte Software zuzugreifen.

Patentansprüche

1. Verfahren zur Ermöglichung eines Zugriffs auf eine geschützte Softwareanwendung durch einen Benutzer eines entfernten medizinischen Diagnosesystems über ein Netz, wobei die geschützte Softwareanwendung bei einer zentralen Anlage gespeichert ist und eine Sicherheitsfreigabe zum Zugriff erfordert, mit den Schritten:
der Benutzer des entfernten Systems überträgt eine Anforderung zum Zugriff über das Netz zu der zentralen Anlage (**160**);
der Benutzer des entfernten Systems überträgt eine Benutzeridentifizierung, ein Kennwort und einen Sicherheitscode über das Netz zu der zentralen Anlage (**164**);
die zentrale Anlage bestimmt, ob das Kennwort und der Sicherheitscode glaubwürdig sind (**166**);
die zentrale Anlage bestimmt, ob der Benutzer des entfernten Systems zum Zugriff auf die geschützte Softwareanwendung befugt ist (**168**); und
dem Benutzer des entfernten Systems wird der Zugriff auf die geschützte Softwareanwendung ermöglicht (**178**), falls das Kennwort und der Sicherheitscode glaubwürdig sind und falls der Benutzer des entfernten Systems dazu befugt ist, auf die geschützte Softwareanwendung zuzugreifen.

2. Verfahren nach Anspruch 1, wobei die zentrale Anlage das von dem Benutzer des entfernten Systems übertragene Kennwort beglaubigt, indem sie das Kennwort mit einem aus einer Gemeinschaftsverwaltungsdatenbank wiedergewonnenen Kennwort vergleicht.

3. Verfahren nach Anspruch 1, wobei die zentrale Anlage den von dem Benutzer des entfernten Systems übertragenen Sicherheitscode beglaubigt, indem sie einen Bezugssicherheitscode gemäß einem Zufallszahlenerzeugungsalgorithmus unter Verwendung einer aus einer Gemeinschaftsverwaltungsdatenbank wiedergewonnenen Keimzahl und Zufallszahlenerzeugungsanfangszeit erzeugt und den Bezugssicherheitscode mit dem von dem Benutzer des entfernten Systems übertragenen Sicherheitscode vergleicht.

4. Verfahren nach Anspruch 1, wobei die Softwareanwendung historische Leistungsdaten für das entfernte medizinische Diagnosesystem umfaßt.

5. Verfahren nach Anspruch 1, wobei die Softwareanwendung eine Hilfseinrichtung zum Vornehmen von Diensten bei dem entfernten medizinischen Diagnosesystem umfaßt.

6. Verfahren nach Anspruch 1, wobei die Softwareanwendung proprietäre Informationen über bei dem entfernten medizinischen Diagnosesystem verwendete

Software umfaßt.

7. Verfahren nach Anspruch 1, wobei die Gemeinschaftsverwaltungsdatenbank Kennwörter und Sicherheitscodes für jede Person speichert, die zum Vornehmen von Diensten bei dem entfernten medizinischen Diagnosesystem und zum Zugriff auf dienstbezogene Anwendungen von dem entfernten medizinischen Diagnosesystem über das Netz befugt ist.

8. Verfahren nach Anspruch 1, wobei der Benutzer des entfernten Systems eine Anforderung zum Zugriff und Benutzeridentifizierungsdaten überträgt, indem er mit einem Web-Browser bei dem entfernten medizinischen Diagnosesystem interagiert.

9. System mit:

einem Netz (**80**);

einem Web-Server (**110**), der mit dem Netz verbunden ist und ein Agenturmodul (**112**) umfaßt, das zur Freigabe eines Zugriffs auf eine geschützte Softwareanwendung im Ansprechen auf eine Genehmigung programmiert ist;

einem entfernten medizinischen Diagnosesystem (**12**) mit einem Web-Browser (**104**) zur Übertragung einer Anforderung zum Zugriff auf die geschützte Softwareanwendung, einer Benutzeridentifizierung, eines Kennworts und eines Sicherheitscodes zu dem Web-Server über das Netz;

einer Gemeinschaftsverwaltungsdatenbank (**116**), die mit jeweiligen Benutzern verbundene Benutzerinformationen, Standortinformationen, mit jeweiligen entfernten medizinischen Diagnosesystemen verbundene Systeminformationen und Vertragsinformationen sowie Genehmigungskriterien umfassende Regeln zur Bestimmung des Zugriffs auf jeweilige geschützte Softwareanwendungen aufweist;

einem Sicherheits-Server (**126**), der zur Beglaubigung des Sicherheitscodes programmiert ist; und

einen Richtlinien-Server (**114**), der mit der Gemeinschaftsverwaltungsdatenbank, mit dem Agenturmodul und mit dem Sicherheits-Server kommuniziert, wobei der Richtlinien-Server zur Beglaubigung des Benutzerkennworts und zur Übertragung der Genehmigung zu dem Agenturmodul, falls das Kennwort und der Sicherheitscode glaubwürdig sind und falls alle Genehmigungskriterien für die geschützte Softwareanwendung erfüllt sind, programmiert ist.

10. System nach Anspruch 9, wobei der Richtlinien-Server zur Ausführung der nachstehende Schritte programmiert ist:

Empfangen der Anforderung zum Zugriff, der Benutzeridentifizierung, des Kennworts und des Sicherheitscodes von dem Agenturmodul;

Wiedergewinnen eines Kennworts und einer Keimzahl, die mit der empfangenen Benutzeridentifizierung verbunden sind, aus der Gemeinschaftsverwaltungsdatenbank;

Bestimmen, ob das wiedergewonnene Kennwort zu dem empfangenen Kennwort paßt; und

Übertragen der wiedergewonnenen Keimzahl zu dem Sicherheits-Server.

11. System nach Anspruch 10, wobei der Sicherheits-Server den empfangenen Sicherheitscode beglaubigt, indem er gemäß einem Zufallszahlenerzeugungsalgorithmus einen Bezugssicherheitscode aus der wiedergewonnenen Keimzahl erzeugt.

12. System nach Anspruch 10, wobei der Richtlinien-Server dazu programmiert ist, zu bestimmen, ob die Benutzeridentifizierung eine Person identifiziert, die zum Zugriff auf die geschützte Softwareanwendung befugt ist, indem er die nachstehenden Schritte ausführt:

Wiedergewinnen der Genehmigungskriterien für die geschützte Softwareanwendung aus der Gemeinschaftsverwaltungsdatenbank;

Wiedergewinnen von Informationen für eine Variable oder mehrere Variablen aus der Gemeinschaftsverwaltungsdatenbank; und

Bestimmen, ob die Variablen die Genehmigungskriterien erfüllen.

13. System nach Anspruch 9, wobei die geschützte Softwareanwendung historische Leistungsdaten (**130**) für das entfernte medizinische Diagnosesystem umfaßt.

14. System nach Anspruch 9, wobei die geschützte Softwareanwendung eine Hilfseinrichtung (**128**) zum Vornehmen von Diensten bei dem entfernten medizinischen Diagnosesystem umfaßt.

15. System nach Anspruch 9, wobei die geschützte Softwareanwendung proprietäre Informationen über bei dem entfernten medizinischen Diagnosesystem verwendete Software umfaßt.

16. System nach Anspruch 9 mit einer Firewall (**138**) zwischen dem Web-Server und dem Richtlinien-Server.

17. System zur Ermöglichung eines Zugriffs auf eine geschützte Softwareanwendung durch einen Benutzer eines entfernten medizinischen Diagnosesystems über ein Netz (**80**), wobei die geschützte Softwareanwendung bei einer zentralen Anlage (**22**) gespeichert ist und eine Sicherheitsfreigabe zum Zugriff erfordert, wobei das entfernte System eine Einrichtung (**104**) zur Übertragung einer Anforderung zum Zugriff auf die geschützte Softwareanwendung, einer Benutzeridentifizierung, eines Kennworts und eines Sicherheitscodes zu der zentralen Anlage über das Netz umfaßt; und wobei die zentrale Anlage eine Einrichtung (**114**, **116**, **126**) zur Bestimmung, ob das Kennwort und der Sicherheitscode glaubwürdig sind, eine Einrichtung (**114**, **116**) zur Bestimmung, ob der Benutzer des entfernten Systems zum Zugriff auf die geschützte Softwareanwendung befugt ist, und eine Einrichtung (**110**, **112**, **114**) zur Ermöglichung des Zugriffs auf die Softwareanwendung für den Benutzer des entfernten Systems, falls das Kennwort und der Sicherheitscode glaubwürdig sind und falls der Benutzer des entfernten Systems zum Zugriff auf die geschützte Softwareanwendung befugt ist, umfaßt.

18. System nach Anspruch 17, wobei die zentrale Anlage eine Einrichtung (**114**) zur Beglaubigung des von dem Benutzer des entfernten Systems übertragenen Kennworts durch einen Vergleich des Kennworts mit einem aus einer Datenbank (**116**) wiedergewonnenen Kennwort umfaßt.

19. System nach Anspruch 17, wobei die zentrale Anlage eine Einrichtung (**126**) zur Beglaubigung des von dem Benutzer des entfernten Systems übertragenen Sicherheitscodes durch eine Erzeugung eines Bezugssicherheitscodes gemäß einem Zufallszahlenerzeugungsalgorithmus unter Verwendung einer aus einer Datenbank wiedergewonnenen Keimzahl und Zufallszahlenerzeugungsanfangszeit und durch einen Vergleich des Bezugssicherheitscodes mit dem von dem Benutzer des entfernten Systems übertragenen Sicherheitscode umfaßt.

20. System nach Anspruch 17, wobei die den Zugriff ermöglichende Einrichtung einen Web-Server (**110**) umfaßt, der zur selektiven Ermöglichung des Zugriffs

auf die geschützte Softwareanwendung im Ansprechen auf die Genehmigung programmiert ist, wobei von dem entfernten medizinischen Diagnosesystem über das Netz auf den Web-Server zugegriffen wird.

Hierzu 7 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

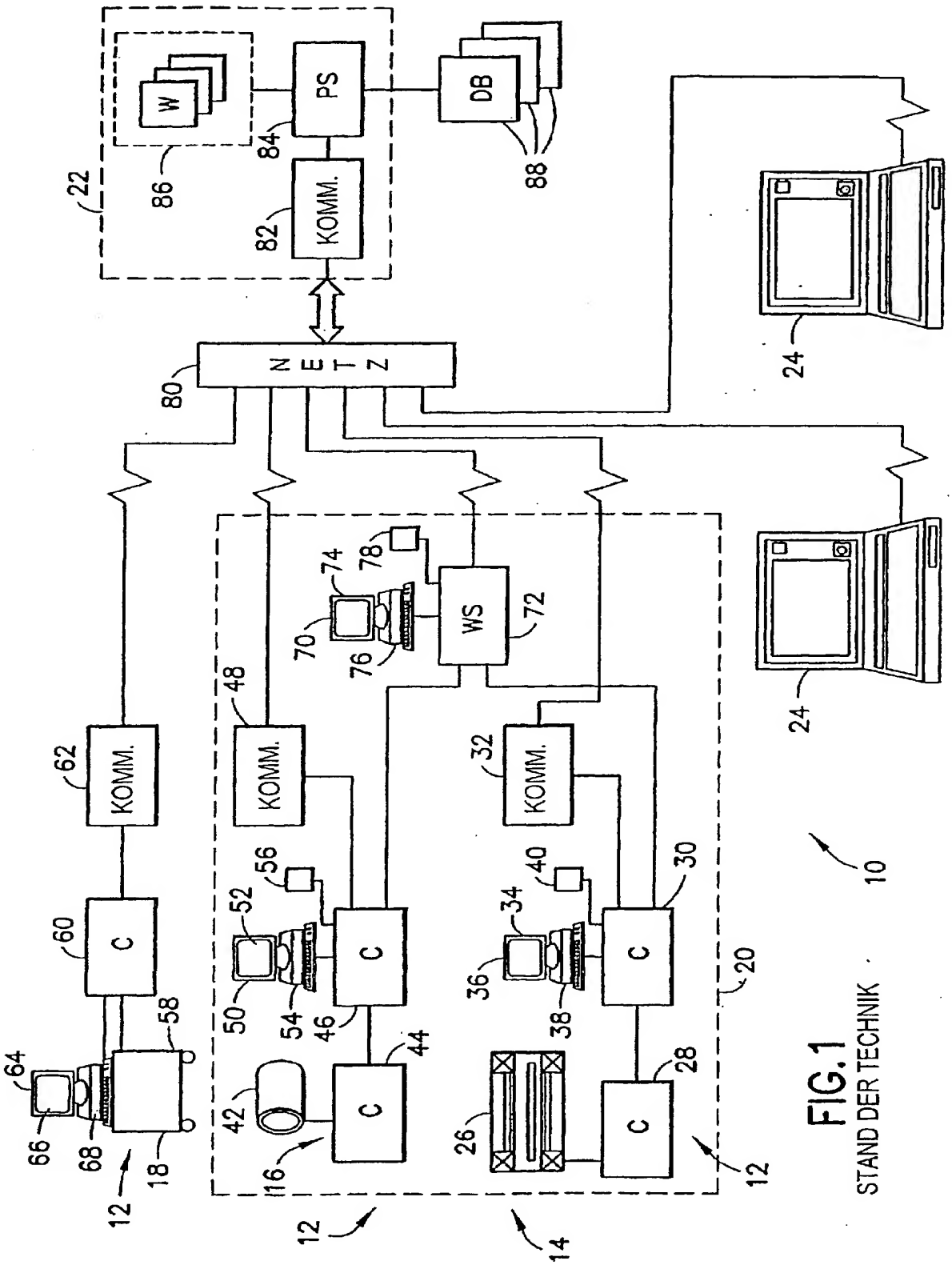


FIG. 1
STAND DER TECHNIK

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

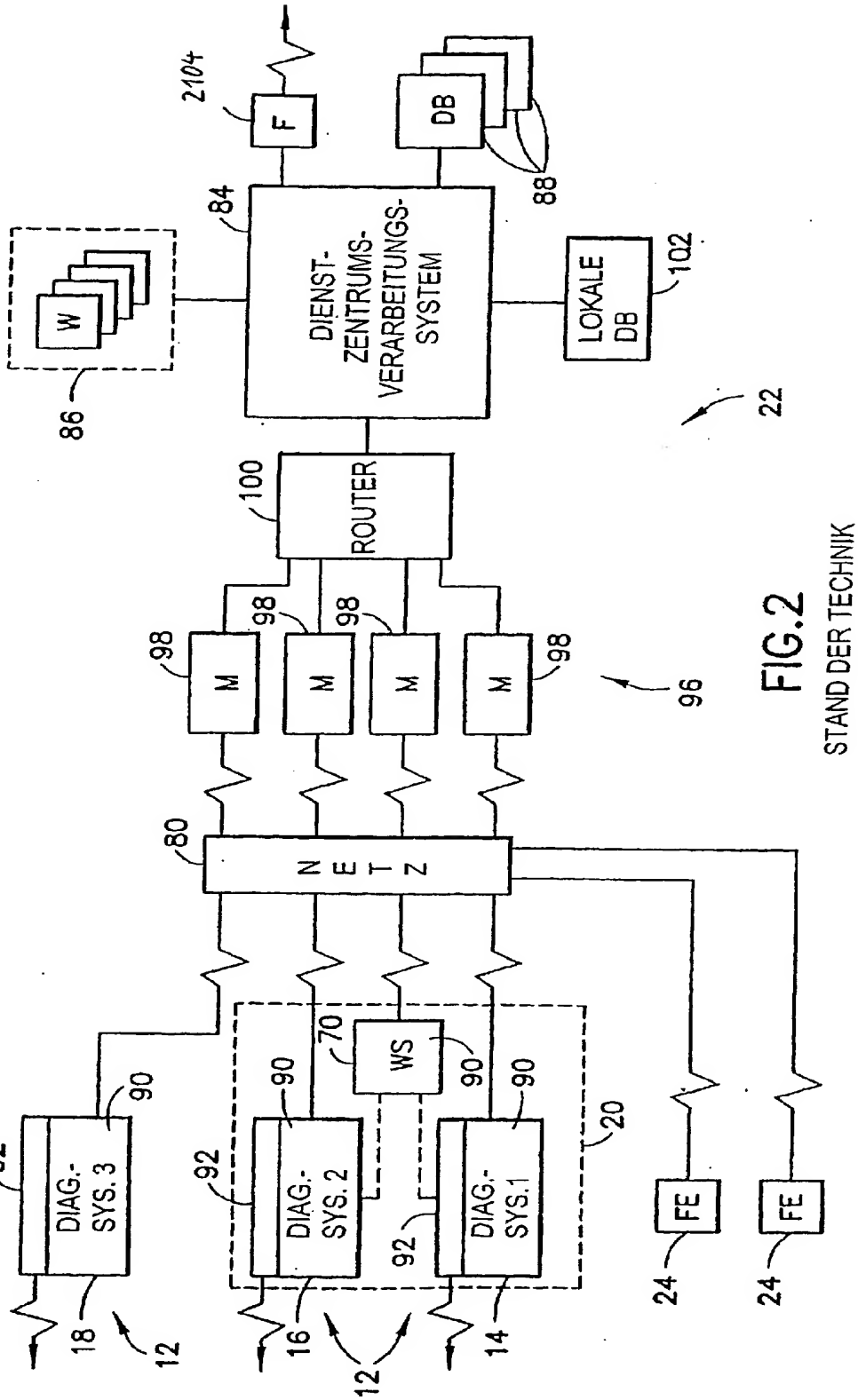


FIG.2
STAND DER TECHNIK

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

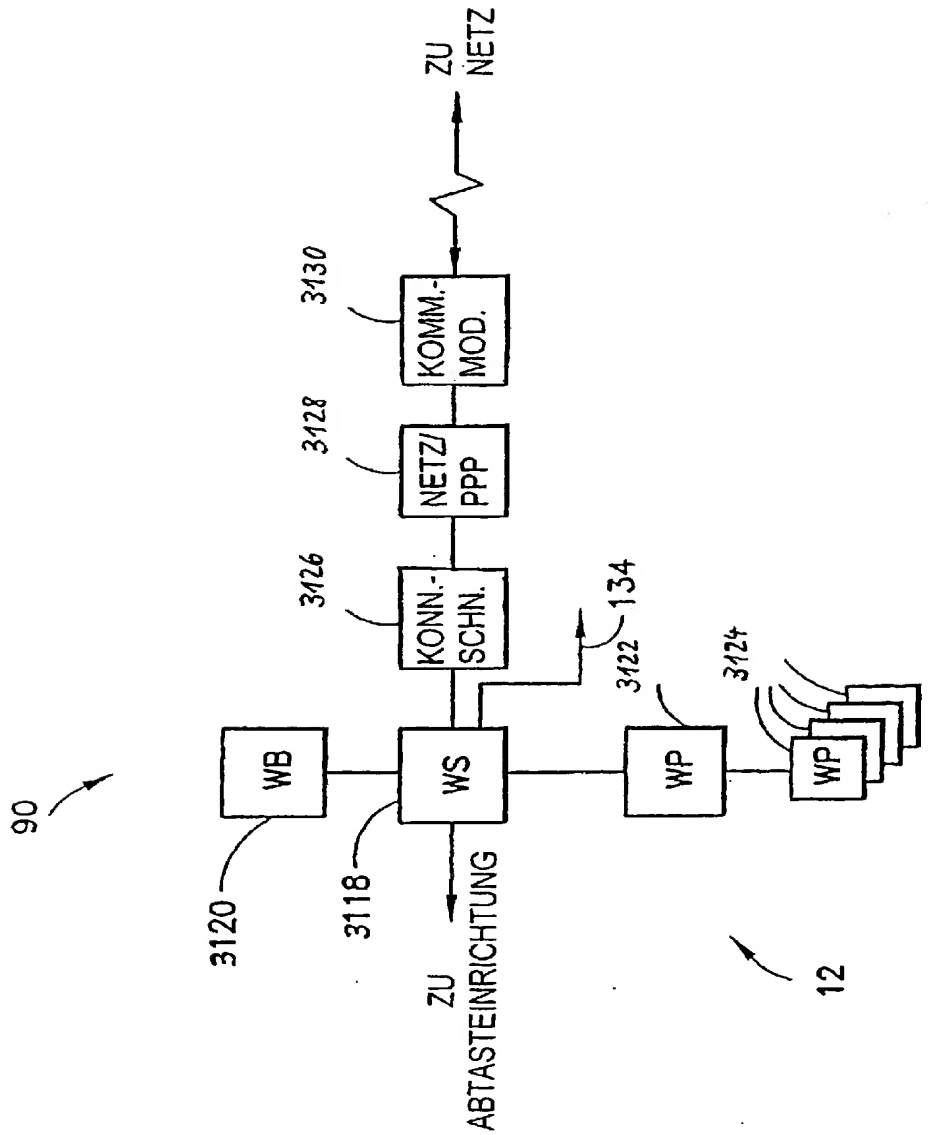


FIG.3

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

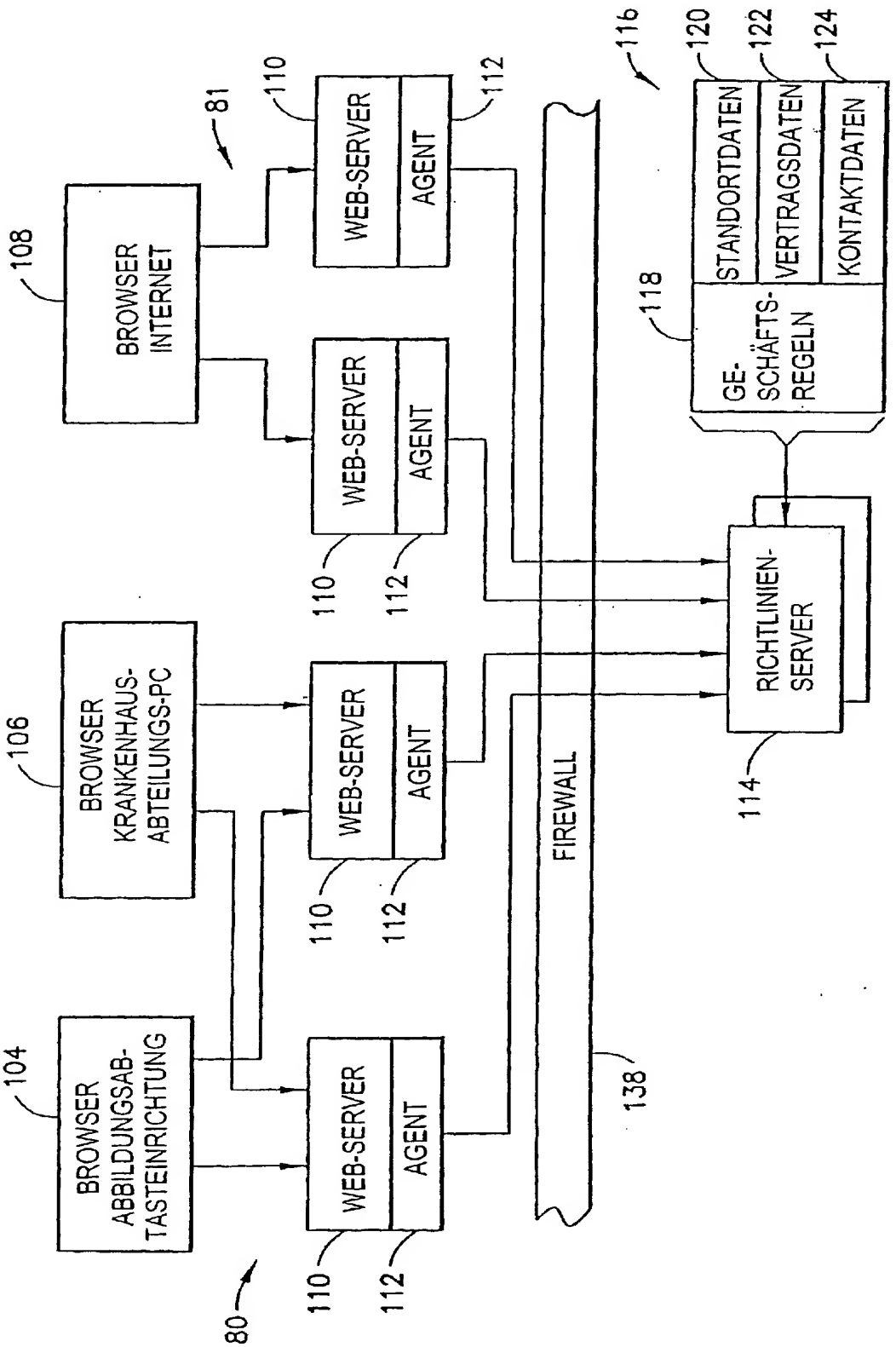


FIG. 4

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

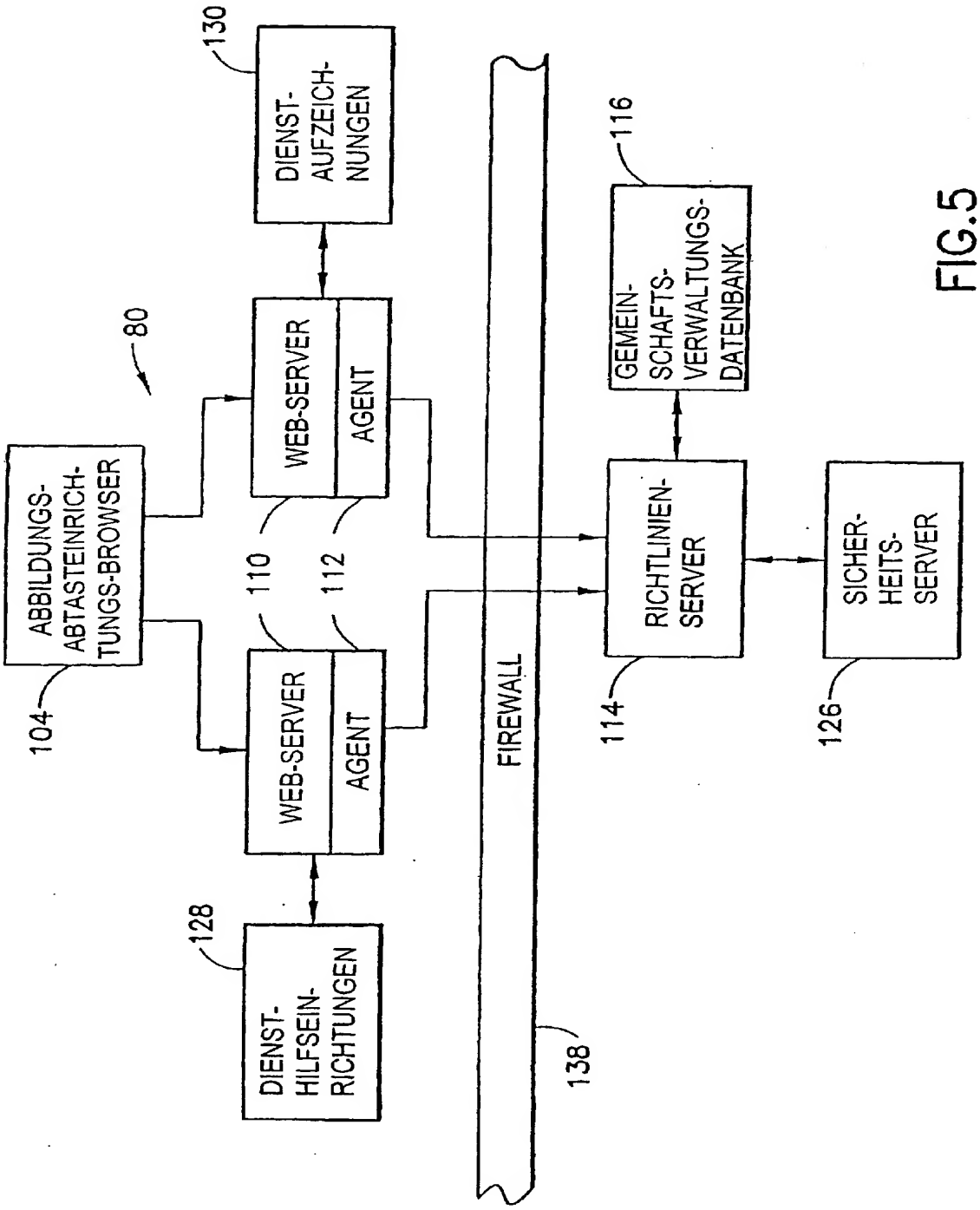


FIG.5

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

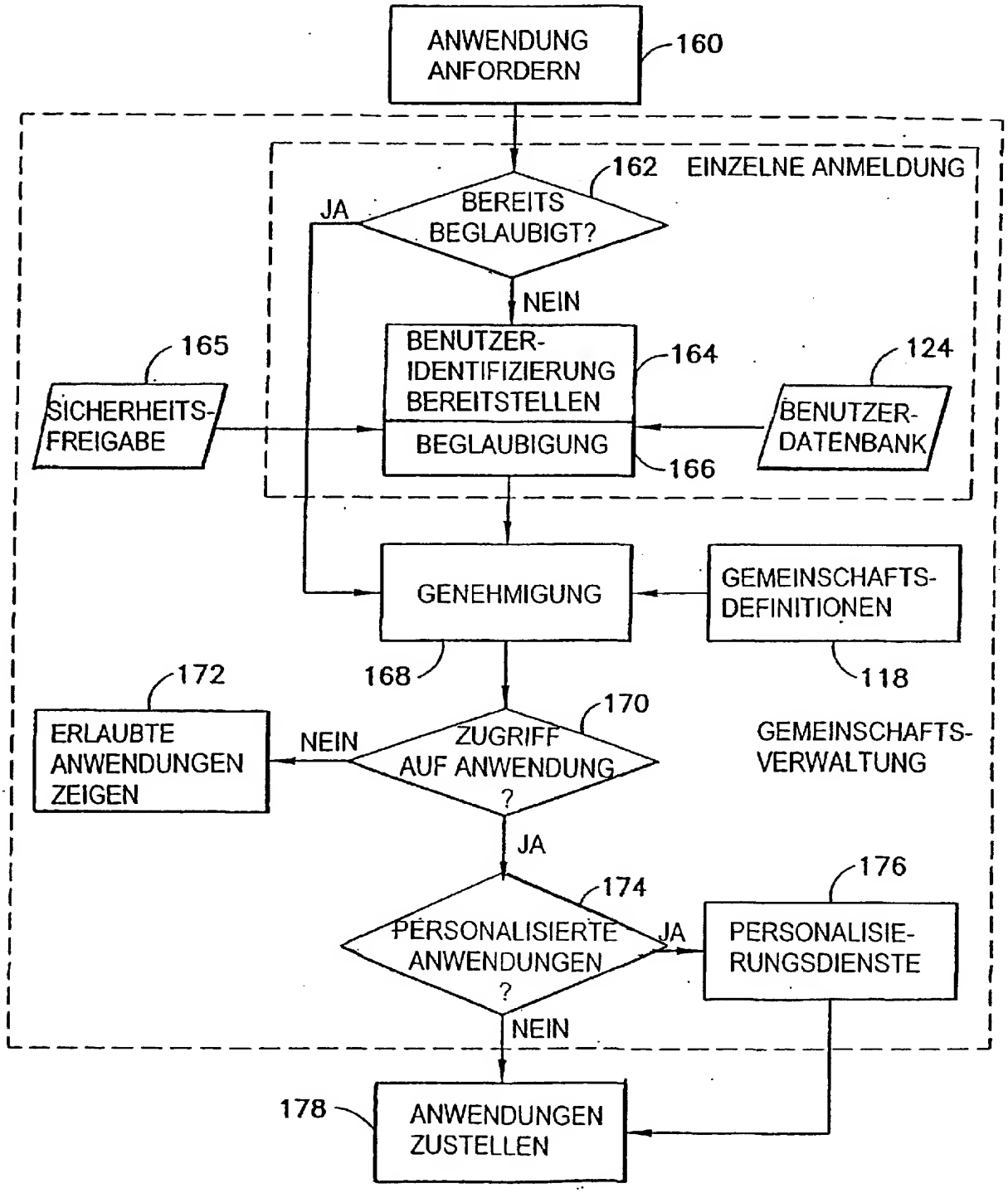


FIG.6

Nummer: DE 100 65 668 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 9. August 2001

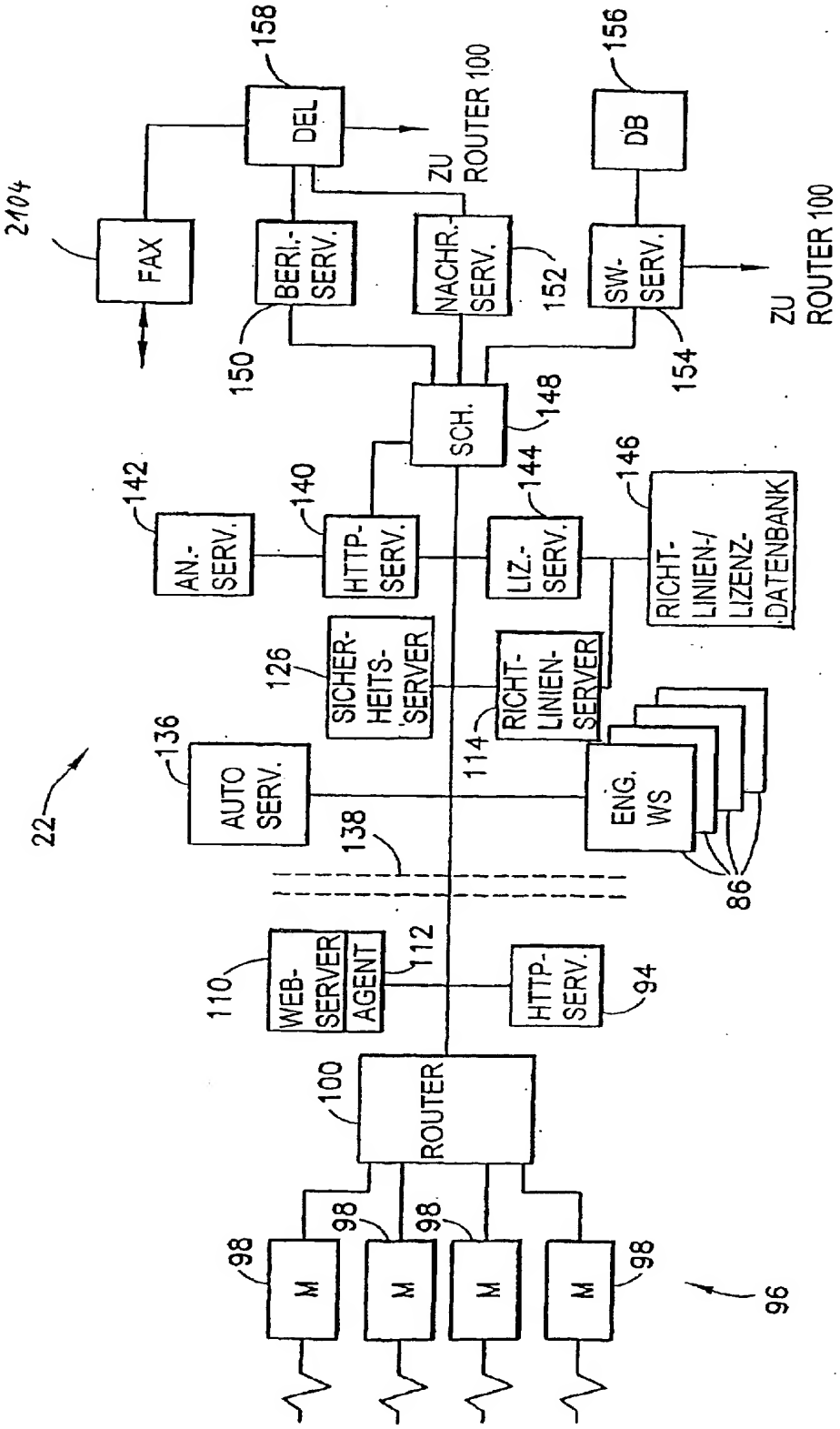
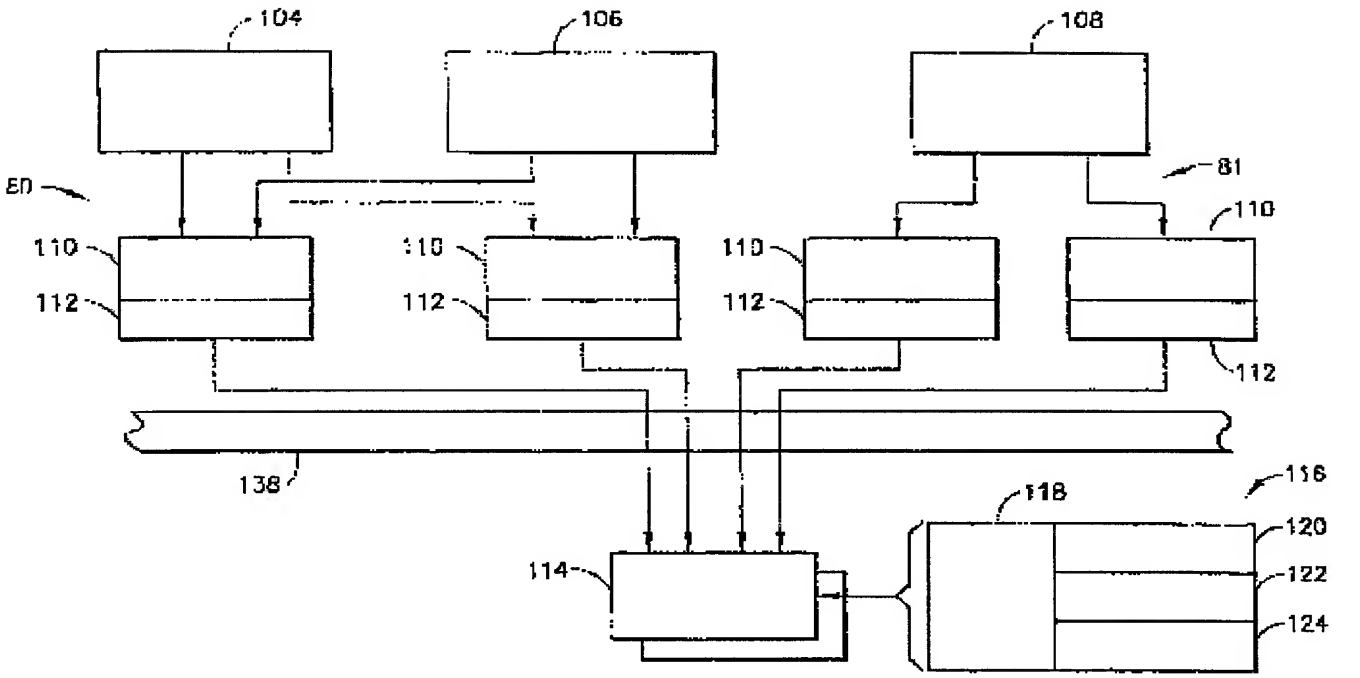


FIG. 7

AN: PAT 2001-531738
TI: Accessing by user distant medical diagnosis system containing protected software application via network by providing authorization certificate to user so that he/she may use protected software application
PN: FR2803462-A1
PD: 06.07.2001
AB: NOVELTY - A central system establishes if a password and a code security are authentic (166) for determining if an approved user of a remote system (168) has reached a protected software application. The authorization certificate is provided to the user so that he/she may use (178) the protected software application on confirmation of the password and the code security. DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for: (a) a system for authenticating a user a software access and/or use by remote user (b) a system for authenticating an access of a remote medical diagnosing system; USE - For accessing by a user of a distant medical diagnosis system via a network using protected software application The latter is stored at the central maintenance level center and requires an authorization certificate for its use. For protecting of software and for controlling software use licences for remote applications. ADVANTAGE - Assures the maintenance of a number of workstations and systems of medical diagnosis operating through a network. DESCRIPTION OF DRAWING(S) - The drawing shows a flowchart of operation of a software security access and/or use by remote user according to the present invention. The drawing includes non-English language text.
PA: (GENE) GE MEDICAL TECHNOLOGY SERVICES;
IN: HUMMEL H J; LAMOUREAUX T L; MEHRING D T; PALLIYAL S M; ZETTEL H A;
FA: FR2803462-A1 06.07.2001; JP2001229130-A 24.08.2001; **DE10065668**-A1 09.08.2001;
CO: DE; FR; JP;
IC: G06F-001/00; G06F-012/00; G06F-012/14; G06F-015/00; G06F-019/00; G06F-159:00; H04L-009/32; H04L-012/24;
MC: S05-G02G1; T01-H01C2; T01-J06A; W01-A05B; W01-A06A;
DC: S05; T01; W01;
FN: 2001531738.gif
PR: US0476594 31.12.1999;
FP: 06.07.2001
UP: 30.10.2001


104
106
108
80
81
110
112
110
112
110
112
110
112
138
116
118
120
122
124
114